PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-319329

(43)Date of publication of application : 16.11.2001

---

(51)Int.Cl. G11B 7/004
G11B 7/007
G11B 19/02
G11B 20/10

---

(21)Application number : 2000-138392 (71)Applicant : TAIYO YUDEN CO LTD

(22)Date of filing : 11.05.2000 (72)Inventor : OMURA YUKIHIDE
SUNAKAWA RYUICHI
SHIMIZU HIRONOBU

---

(54) RECORDER FOR WRITE ONCE OPTICAL DISK, AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To contrive the discrimination of a write once optical disk of a specified manufactures from other write once optical disks by giving the security function to this write once optical disk only when it is used.

SOLUTION: In the recorder for the write once optical disk provided with the user's area for writing user data and the system area utilized by the system when at least this writing operation is performed, the information for the countermeasure as to the security is written into a part of the system area when the manufacture of the above write once optical disk is checked up and found to be the specified manufacturer

(thereby the write once optical disk is produced: 'support disk' in figure 8). Only for the write once optical disk produced by the specified manufacturer, the information for the measure as to the security is written into a part of the system area.

LEGAL STATUS [Date of request for examination] 02.10.2003
[Date of sending the examiner's decision of rejection] 12.06.2006
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The recording apparatus for write-once mold optical disks characterized by having investigated the manufacturer information recorded on the interior of said write-once mold optical disk electronically refreshable in the recording apparatus equipped with the system area used by the system in case the write-in actuation concerned is performed at least with the user area for writing in user data for write-once mold optical disks, and writing the information for security countermeasures in said a part of system area when it is predetermined manufacturer information.

[Claim 2] Said system area is a recording device for write-once mold optical disks according to claim 1 characterized by being a field for laser on-the-strength calibrations at the time of writing in user data.

[Claim 3] Said system area is a recording device for write-once mold optical disks according to claim 1 characterized by being either of the fields for specifying the termination location of the field for session information storing referred to in case the user data written in the field for temporary storages of the session information at the time of writing in user data or the user area are reproduced, or a user area.

[Claim 4] The information for said security countermeasures is a recording device for write-once mold optical disks according to claim 1 characterized by being the identification information for solid-state discernment of said write-once mold optical disk.

[Claim 5] The information for said security countermeasures is a recording device for write-once mold optical disks according to claim 1 characterized by being the identification information for user authentication.

[Claim 6] The information for said security countermeasures is a recording device for write-once mold optical disks according to claim 1 characterized by being the key information for enciphering said user data.

[Claim 7] The information for said security countermeasures is a recording device for write-once mold optical disks according to claim 1 characterized by being the key information for decoding the encryption data written in said user area.

[Claim 8] An access means to access a write-once mold optical disk, and the read-out means which reads manufacturer information from said write-once mold optical disk through said access means, A judgment means to judge whether the manufacturer information read by said access means is predetermined manufacturer

information, The recording device for write-once mold optical disks characterized by having the write-in means which writes the information for security countermeasures in the system area of said write-once mold optical disk when the judgment result of said judgment means is not no.

[Claim 9] An access means to access a write-once mold optical disk, and the read-out means which reads manufacturer information from said write-once mold optical disk through said access means, A judgment means to judge whether the manufacturer information read by said access means is predetermined manufacturer information, The record medium characterized by storing the program for realizing the write-in means which writes the information for security countermeasures in the system area of said write-once mold optical disk when the judgment result of said judgment means is not no.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the recording device for write-once mold optical disks, and a record medium. It is related with the recording device and record medium which are applied to the write-once mold optical disk represented in detail by CD-R (Compact Disc Recordable) which can write in data only once.

[0002]

[Description of the Prior Art] As a distribution medium of electronic data, such as various contents and a computer program, CD-ROM (Compact Disc Read Only Memory) is used abundantly. although CD-ROM is a duplicate object manufactured by press molding etc. from the master CD which recorded electronic data and it is mainly used for the media of extensive distribution -- little sample version CD and private CD of the number of distribution (the number of manufactures) -- the optical disk unit of a write-once mold -- CD-R is used typically. CD-R has the difference in CD-ROM and structure between transparent disk substrates and reflecting layers (detailed structure is mentioned later.) in that it has the recording layer which consists of organic coloring matter, irradiates high power laser at the recording layer concerned using the recording device (CD-R writer) of dedication, and can record information in a user phase by forming an information pit in the recording layer concerned by the thermal reaction.

[0003] CD-R is the write-once (postscript is possible) mold which cannot perform informational elimination or overwrite as above-mentioned. That is, informational elimination and informational rewriting which were written in once are impossible. Therefore, it is a storage indispensable to applications, such as storage of electronic data which requires especially maintenance, and distribution, from having the outstanding advantage that informational elimination and the informational alteration by the inaccurate person can be prevented certainly.

[0004]

[Problem(s) to be Solved by the Invention] (1) However, if it was in the conventional write-once mold optical disk, although there was an outstanding advantage that elimination and an alteration of recording information could be prevented, since read-out of recording information was free, there was un-arranging [that unjust read-out or the illegal copy of recording information could not be prevented]. For this reason, storage of CD-R which recorded the information which requires secrecy is faced. Although a strict management regulation must be applied, employment of such a management regulation is considerable difficulty. As a result of in many cases being easy to flow in an easy inclination and being able to prevent carrying out of CD-R and read-out of information by the indiscreet person neither from the inconsistency of a regulation, nor tameness, there was a trouble that the external outflow of the information which should be kept secret, or the appearance of CD-R copied unjustly was nonavoidable. In addition, although this trouble is being able to say the general storage device of not only CD-R but a portable mold, it is serious about especially CD-R. Actually, in addition, CD-R is because unjust reading of the recording

information is possible also even for after no more use, unless CD-R which is widely used for distribution, storage, etc. of electronic data which require maintenance taking advantage of the write-once type of the description and which became unnecessary is destroyed physically (for example, a blemish is given or cut intentionally).

[0005] (2) Moreover, although information is recorded in a user phase by irradiating high power laser at a recording layer, and forming the information pit by the thermal reaction if it is in the conventional write-once mold optical disk, for example, CD-R Formation of an information pit may go wrong (write-in failure), or even if it is able to form an information pit rarely, the formation is insufficient, and an error may be generated in case it is read-out (read-out failure). Especially such a trouble may be experienced when a no brand article is used. It is because the manufacturer responsibility for a no brand article is generally indefinite and existence of CD-R of inferior quality cannot be denied compared with a normal article (what specified the manufacturer). If such a background is taken into consideration, use of a normal article should be ideally recommended to the user, but there are fairly many users of a no brand article, and although it is a part, generating of the above-mentioned trouble resulting from existence of a crude article poses a problem from the reasons of a no brand article being able to come to hand cheaply compared with a normal article in fact.

[0006] therefore, the case where a predetermined manufacturer's write-once mold optical disk is used for the technical problem which this invention tends to solve -- the write-once mold optical disk -- security nature -- it can give -- with -- **** -- it is shown in attaining differentiation with the other write-once mold optical disk.

[0007]

[Means for Solving the Problem] In case the recording apparatus for write-once mold optical disks according to claim 1 performs the write-in actuation concerned at least with the user area for writing in user data, it is characterized by having investigated the manufacturer information recorded on the interior of said write-once mold optical disk electronically refreshable, and writing the information for security countermeasures in said a part of system area, when it is predetermined manufacturer information in the recording apparatus equipped with the system area used by the system for write-once mold optical disks. According to this, the information for security countermeasures is written in a part of the system area only about the write-once mold optical disk made by the predetermined manufacturer.

[0008] The recording apparatus for write-once mold optical disks according to claim 2 is characterized by said system area being a field for laser on-the-strength

calibrations at the time of writing in user data in the recording apparatus for write-once mold optical disks according to claim 1. According to this, the information for security countermeasures is written in the specific field (field for laser on-the-strength calibrations) to which the existence is disregarded at the time of playback of data.

[0009] The recording apparatus for write-once mold optical disks according to claim 3 is characterized by said system area being either of the fields for specifying the termination location of the field for session information storing referred to in case the user data written in the field for temporary storages of the session information at the time of writing in user data or the user area are reproduced, or a user area in the recording apparatus for write-once mold optical disks according to claim 1. According to this, the information for security countermeasures is written in the field to which access with all direct from a user is not permitted.

[0010] The recording apparatus for write-once mold optical disks according to claim 4 is characterized by the information for said security countermeasures being the identification information for solid-state discernment of said write-once mold optical disk in the recording apparatus for write-once mold optical disks according to claim 1. According to this, the security countermeasures based on solid-state discernment of a write-once mold optical disk become possible.

[0011] The recording apparatus for write-once mold optical disks according to claim 5 is characterized by the information for said security countermeasures being the identification information for user authentication in the recording apparatus for write-once mold optical disks according to claim 1. According to this, the user authentication using the information for security countermeasures becomes possible.

[0012] The recording apparatus for write-once mold optical disks according to claim 6 is characterized by the information for said security countermeasures being the key information for enciphering said user data in the recording apparatus for write-once mold optical disks according to claim 1. According to this, the user data encryption using the information for security countermeasures becomes possible.

[0013] The recording apparatus for write-once mold optical disks according to claim 7 is characterized by the information for said security countermeasures being the key information for decoding the encryption data written in said user area in the recording apparatus for write-once mold optical disks according to claim 1. According to this, the decode using the information for security countermeasures of encryption data is attained.

[0014] The recording device for write-once mold optical disks according to claim 8 An

access means to access a write-once mold optical disk, and the read-out means which reads manufacturer information from said write-once mold optical disk through said access means, A judgment means to judge whether the manufacturer information read by said access means is predetermined manufacturer information, When the judgment result of said judgment means is not no, it is characterized by having the write-in means which writes the information for security countermeasures in the system area of said write-once mold optical disk. According to this, the information for security countermeasures is written in the system area only about the write-once mold optical disk made by the predetermined manufacturer.

[0015] An access means by which a record medium according to claim 9 accesses a write-once mold optical disk, The read-out means which reads manufacturer information from said write-once mold optical disk through said access means, A judgment means to judge whether the manufacturer information read by said access means is predetermined manufacturer information, When the judgment result of said judgment means is not no, it is characterized by storing the program for realizing the write-in means which writes the information for security countermeasures in the system area of said write-once mold optical disk. According to this, said access means, a read-out means, a judgment means, and a write-in means are realized by organic association with the hardware property and this program containing a microcomputer.

[0016]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail with reference to a drawing. In addition, instantiation of the notation of the specification thru/or example and numeric value of various details in the following explanation, or a character string and others is reference to the last for making thought of this invention clear, and it is clear that its the thought of this invention is not limited by those all or parts. Moreover, although the explanation covering the details is avoided about the well-known technique, a well-known procedure, well-known architecture, and well-known circuitry (following "common knowledge matter"), this is also for giving explanation brief and does not eliminate intentionally all or a part of these Governor Shu term. Since it is this the Shu Governor term at the application time of this invention and this contractor can just be going to know it, naturally it is contained in the following explanation.

[0017] Drawing 1 is the external view (a) and its important section enlarged drawing (b) of a write-once mold optical disk (henceforth "CD-R"). Setting to these drawings, CD-R1 is the diameter of 12cm (there is also a thing with a diameter of 8cm.).

Hereafter, it is a thing with a diameter of 12cm and explains. It has the shape of a disk and with a diameter of 15mm center hall 1a is formed in the core of a disk. The distance from the core T0 of a disk to the wall (disk common-law marriage T1) of center hole 1a 7.5mm, The distance from T0 to the disk rim T7 is 60mm. Among these T1-T7 Two or more concentric record sections, That is, they are PCA (Power Calibration Area), PMA (Program Memory Area), and a lead-in groove (it has abbreviated to "RI" by a diagram.) to the order from the inner circumference side of a disk. Data area (it has abbreviated to "UA" by a diagram.) And lead-out (it has abbreviated to "RO" by a diagram.) Each field is prepared.

[0018] When each field is outlined, PCA located in T2 - T3 is a trial writing field for the laser adjustment on the strength performed in case data are recorded on CD-R1. Generally about 100 times of this trial writing are possible, and it consumes the field of one batch by at least 1 time of data logging. PMA located in T3 - T four is a field where the track number and initiation/termination location are saved temporarily, when there is a truck of the session which is not closed yet by CD-R1. The lead-in groove (RI) located in T-four-T5 is a field in the head (inner circumference side of a disk) of a session truck, and is a field where TOC (the number of trucks currently recorded on Table Of Contents:CD, a starting position, and the die length of the sum total of a data area) of a session is saved. A closing of a session writes the information saved at PMA temporarily in this lead-in groove (RI).

[0019] The data area (UA) located in T5-T6 is a field in which data are actually written in a user phase. The storage capacity of data is about 680 M bytes (a thing with a diameter of 8cm is about 190 M bytes of max) of max, and if this storage capacity is expressed with sound recording time amount, it will become in the maximum about 74 minutes (a thing with a diameter of 8cm is the maximum about 21 minutes). a data area (UA) is managed by the logical block of the predetermined size (2 K bytes) unit which continues from immediately the back of a lead-in groove (RI) -- having -- coming -- **** -- every logical block -- the max from 0 -- LBN (Logical Block Number) to about 330000 is assigned. The lead-out (RO) located in T6-T7 is a field in the last (periphery side of a disk) of a session, and is a field which shows that the last of a data area (UA) was reached.

[0020] The location on the disk of each [these] field is standardized except for T3. That is, the location where T2 separated from T0 22.5mm, the location where T four separated from T0 23mm, the location where T5 separated from T0 25mm, and T6 are prescribed to become the location distant from T0 58mm. In addition, this is the convenience of illustration although the same sign (T7) shows the disk rim and the

termination location of lead-out (RO) by a diagram. The actual termination location of lead-out (RO) turns into a location distant from T0 58.5mm. The following, as long as there is no notice, T7 shall express the termination location of lead-out (RO). Incidentally, initiation and the termination location (T6 and T7) of lead-out (RO) change according to the amount of the data recorded on CD-R1. The above-mentioned actual value (T6=58mm, T7=58.5mm) is a thing when making the amount of stored data into max.

[0021] Drawing 2 is cross-section structural drawing of CD-R1. CD-R1 is transparent, on substrate 1b which consists of an ingredient (for example, plastics) which was excellent in thermal resistance, moisture resistance, and a moldability, and was equipped with necessary optical properties (a refractive index, birefringence, etc.), carries out the laminating of the protective layer 1e which consists of hard material, such as 1d of reflecting layers, resin, etc. which consist of metallic materials, such as recording layer 1c which consists of organic coloring matter, and aluminum, and is formed. The thickness of the whole cross section is 1.2mm.

[0022] The point that the point of having recording layer 1c, and 1f of spiral guide rails called a wobbles groove between recording layer 1c and substrate 1b are formed has the difference in structure with CD-ROM. Record of the data to CD-R1 irradiates the powerful laser for record along with 1f of guide rails from the background of substrate 1b, and is performed by heating recording layer 1c and forming an information pit (pit: a part for the physical deformation affected zone for modulating the laser reflected light for playback).

[0023] Drawing 3 is the mimetic diagram showing 1f (wobbles groove) of guide rails of CD-R1. As 1f of guide rails is shown in this drawing (a), it is continuously formed toward the periphery side (from a periphery side to or an inner circumference side) in the way of a picture drawn without lifting the brush from the paper from the inner circumference side of a disk, and the width of face of 1f of guide rails is about 0.5-0.7 micrometers, and spacing is about 1.6 micrometers. Data logging in a user phase is performed along with 1f of guide rails by forming an information pit in recording layer 1c of a guide rail 1f (or Hazama's land of 1f of guide rails) directly under. In addition, although it sees from the background of CD-R1, a part for a land (crest) and a crevice is called groove (trough) for a part for heights of 1f of guide rails and the part of a trough is generally called wobbles group, a crest and a trough are not distinguished on these specifications.

[0024] Here, the role of 1 of 1f of guide rails is to hold the timing information for controlling the rotational speed of a disk at the time of data logging of a user phase.

For this role, 1f of guide rails is formed in the configuration which moves in a zigzag direction the predetermined period T1 (for example, period with which T1 is equivalent to 22.05kHz) (it is also called "wobbling".), as shown in this drawing (b). At the time of record of data, the optical pickup at the time of data logging and the relative velocity between disks are kept constant by tracing this meandering by the optical pickup, detecting a period T1, and controlling the rotational speed of a disk so that that detection period T1 becomes fixed.

[0025] Other roles of 1f of guide rails are to hold various disk information including the positional information of each record section on a disk (PCA, PMA, RI, UA, and RO). Disk information is also called ATIP (Absolute Time In Pregroove: call it a common name "A chip".), and while various information other than the above-mentioned positional information, such as the record laser reinforcement and disk rotational speed of criteria, an application code, or a disk type, is included, the information (henceforth "manufacturer information") that the manufacturer of a disk can further be specified is also included in ATIP. For example, since the starting position information on a lead-in groove (RI) differs for every manufacturer of a disk, it can use this starting position information as manufacturer information.

[0026] As shown for example, in this drawing (c), 1f of actual guide rails moves in a zigzag direction still more finely (or deformation), and they have multiplexed ATIP information with the period T2 of the thin meandering. While carrying out the separation extract of timing information and the ATIP information using the periodic (frequency) difference at the time of record of data and performing the roll control of a disk using timing information, it becomes possible to control a data-logging location etc. using ATIP information.

[0027] In addition, in the example of illustration, although ATIP information is multiplexed with the thin meandering period T2 of 1f of guide rails, it is not limited to this mode. It is also possible to form parts for a physical unique variant part, such as irregularity, in the side attachment wall of 1f of guide rails, and to reproduce ATIP information from spacing for the unique variant part etc. that what is necessary is to trace 1f of guide rails and just to be able to reproduce ATIP information from the trace signal in short at the time of record of data. Hereafter, ATIP information shall be multiplexed by the above-mentioned thin meandering period T2 on account of explanation.

[0028] Drawing 4 is a block diagram of a manufacturing installation 10 used mainly in the manufacture phase of a disk, in order to form 1f of guide rails in CD-R1. The 1st wobbling signal generating circuit 11 in which a manufacturing installation 10

generates the wobbling signal for synchronizing signals (henceforth a "synchronous wobbles signal") in this drawing based on the timing information of a period T1, The 2nd wobbling signal generating circuit 12 which generates an ATIP wobbles signal based on the ATIP signal which includes the manufacturer information on a disk at least, The 1st optical modulator 15 which modulates the laser beam which incorporated the synchronous wobbles signal through the 1st amplifier 13, and was discharged from the non-illustrated laser light source using this synchronous wobbles signal, The 2nd optical modulator 16 which modulates the laser beam which incorporated the ATIP wobbles signal through the 2nd amplifier 14, and passed the 1st optical modulator 15 using this ATIP wobbles signal, The mirror 17 which reflects the laser beam which passed the 2nd optical modulator 16, and the objective lens 18 which narrows down the laser beam reflected by the mirror 17, and irradiates the recording surface of CD-R1, 1f of curled form guide rails shown in drawing 3 (a) is formed by carrying out the rotation drive of CD-R1 concerned, having the motor 19 which carries out the rotation drive of CD-R1, and moving the exposure location to the recording surface of the above-mentioned laser beam to radial [of CD-R1].

[0029] Here, the laser beam which passed the 1st optical modulator 15 has received the modulation by the synchronous wobbles signal, and the laser beam which passed the 2nd optical modulator 16 further has received the modulation by the ATIP wobbles signal. That is, a laser beam will be modulated two convenience. Therefore, as "wobbling" (meandering) of the 1f of the guide rails formed in the recording surface of CD-R1 will be carried out corresponding to the synthetic period of the period T1 of a synchronous wobbles signal, and the period T2 of an ATIP wobbles signal and they are shown in drawing 3 (c) after all, the synthetic meandering configuration of having two periods (T1, T2) is acquired.

[0030] Drawing 5 is the format conceptual diagram of each record section of CD-R1. In this drawing, PCA, PMA, a lead-in groove (RI), a data area (UA), and lead-out (RO) correspond to the same name part in drawing 1 (b), respectively. Although especially the size (information write-in possible capacity) of PCA and PMA is not decided, about 3.5 M bytes is secured by the initial complement corresponding to the above-mentioned count of trial writing (generally about 100 times), or the count of temporary storage of session information, for example, PCA, and the capacity of about 2 M bytes is secured by PMA. Incidentally, the starting position (T2) of PCA and the starting position (T3) of PMA can be expressed in writing from such instantiation capacity with the location for "T2=T-four-about 35 seconds", and the location for "T3=T-four-about 13 seconds" on the basis of the starting position (T four) of the

standardized lead-in groove (RI).

[0031] Since it is a trial writing field at the time of PCA performing data logging, and the field which stores temporarily the session information by which PMA is not closed as stated above, these two fields (PCA/PMA) are fields used only at the time of data logging (access). On the other hand, since it is the field which records as TOC the session information by which the lead-in groove (RI) was closed, the field where, as for a data area (UA), data are actually written in, and the field where lead-out (RO) specifies the end of a data area, these three fields (a lead-in groove / data area / lead-out) are fields used at both times of data logging and playback (access).

[0032] On the other hand, if all these fields are seen in respect of the access ease from a user that is The reader of CD-R1 If it evaluates in respect of the ability of the contents of storage to be easily accessed using the usual tools (file system on the operating system typically carried in the personal computer concerned etc.) from users, such as a personal computer which it had Although complete grasp of the contents of storage is possible though natural about a data area (UA), contents grasp of other fields (PCA, PMA, a lead-in groove, and lead-out) is impossible.

[0033] Of course, since such a tool is difficult to receive for a general user, if it is possible if a special tool is used, but use of the exceptional tool to apply is removed, it can be said that other fields other than a data area (PCA, PMA, a lead-in groove, and lead-out) are special fields where only access from a system was permitted. Hereafter, this special field is called "system area" and the thing of the field where access from a user was permitted is made a "user area." That is, a user area, other PCA, PMA, a lead-in groove (RI), and lead-out (RO) of a data area (UA) are system areas.

[0034] Now, the point of CD-R1 in the gestalt of this operation In case data logging is performed in ** user phase so that it may mention later, the manufacturer (manufacturer information currently written in CD-R1) of CD-R1 is questioned. When the manufacturer (manufacturer information) is indicated by the predetermined support list, it is the solid-state identification information (it is called "ID information" below.) of CD-R1 in a part of system area of CD-R1 concerned. It is in the point which wrote in predetermined cryptographic key information. ** Use a cryptographic key at the time of data logging, encipher record data again, and be in the point which wrote the encryption data concerned in CD-R1 concerned. ** In case the data playback and the disk copy of CD-R1 which recorded encryption data are performed further, be in the point of having been made to perform user authentication based on said ID information.

[0035] Security nature can be given now to the management and distribution of data

which require secrecy with the point of these **s - **. That is, with (**) which enciphers data and can be recorded on CD-R1, in case this encryption data is reproduced (decode), user authentication using ID information can be performed and data playback can be permitted only to (**) and a registered user (user who knows ID information).

[0036] This security function is a function which is not added to CD-R1 from the beginning, and is added when some conditions are fulfilled. that is, since it is the restrictive function by which (**) addition is carried out and in other words is the function which is not added to a manufacturer's (or a manufacturer -- unknown) CD-R which is not indicated by the support list only when the manufacturer of CD-R1 is indicated by the predetermined support list, differentiation of CD-R can be attained by the existence of this function.

[0037] As the beginning explained, CD-R1 with a user available in a commercial scene is divided into the normal article which specified the manufacturer, and the other non-normal article (no brand article). Although a no brand article is a low price, since it was not able to deny existence of a crude article, although it was rare, normal data logging might be unable to be performed. Although management and the distribution application of important data should have been especially forced into use of a normal article, since such compulsion was difficult in practice, it was not able to deny the possibility of troubles, such as a data write-in failure accompanying use of a no brand article, and read-out failure.

[0038] CD-R1 in the gestalt of this operation can use the security function of the above [a user] now by using a manufacturer's CD-R1 indicated by the user list. Since the above-mentioned security function cannot be used when the no brand article which is not indicated by the user list is used if it puts in another way When applying to the storage and distribution of data which require especially secrecy, a user cannot but stop using a normal article and eliminates use of a no brand article as a result. The merit according to rank that the trouble of the write-in failure and read-out failure of record data resulting from a crude article is avoidable is obtained.

[0039] Although it is desirable to have a unique value (value not overlapping) covering the total number of manufactures of CD-R1 as for ID information written in the system area of CD-R1, since there is concern whose information bit forms many bits and presses the storage capacity of a system area when the number of manufactures becomes huge, it is good also as different information for every manufacture lot, every production line, and every manufacture stage. This ID information is used for access collating to CD-R1 at the time of performing data playback and a data copy so that it

may mention later. The input of ID is required with the application which performs playback of data etc., coincidence with inputted ID and ID currently written in the system area is judged, and, only in coincidence, access is permitted. The playback and the duplicate of data by the inaccurate user (user who does not know ID) can be prevented by this, and the outflow of data and the appearance of an inaccurate product can be avoided.

[0040] The acquisition approach of ID information can consider the following two things. A primary method puts the piece of paper which printed ID information into the package of CD-R1, and ships it together. A user inputs ID information, looking at the piece of paper. This approach is a most certain and easy approach, unless it is similar with the install registration approach currently generally performed in the field of the software package and a piece of paper is lost. In addition, as deformation of this approach, although ID information may be printed on the front face and label of a package, all are the same at the point of sending CD-R1 and ID information suitable together to a user. In the second approach, ID information comes to hand from the predetermined website on the Internet. This website is a dynamic website constituted so that ID information unique about CD-R by all manufacturers could be published, can answer ID information issue demand from a user, and can deliver suitable ID information to the addressing to a user concerned. Such a website can be built in the combination of server side script engines, such as ASP (Active Server Pages) which operates for example, on a WWW server, and CGI (Common Gateway Interface), and a database. In this case, it is desirable to put the piece of paper which printed beforehand the code information for registration (code information which shows the identification information of a manufacturer exception or others) into the package of CD-R. A user demands handing out of ID information using this code information. A website registers into a database the code information and delivered ID information that it was inputted, and manages them. Furthermore, the second approach can also be developed as follows. The user-identification information only for the users is used for first-time ID information issue demand, reception and the user concerned use the user-identification information for subsequent ID information issue demands from a website, and a user accesses a website. If it does in this way, a website becomes possible [performing hysteresis management of delivered ID information for every (every / namely, / user) user-identification information], and a user can access a website and can see the hysteresis information on ID information used in the past at any time. Therefore, for a user, the merit that it is not necessary to carry out hysteresis management by oneself is obtained.

[0041] The key information written in a system area together on the other hand is used in order to encipher the raw data written in a data area in a user phase. That is, after reading a cryptographic key with the application which records data and changing raw data into encryption data using this cryptographic key, that encryption data is written in the data area of CD-R1. Also in case this cryptographic key decodes encryption data, it is used. That is, the input of ID is required with the application which reproduces data at the time of playback of data, coincidence with inputted ID and ID currently written in the system area is judged, in coincidence, a cryptographic key and encryption data are read, encryption data are decoded using the cryptographic key, it changes into raw data, and use of a user is presented.

[0042] Therefore, the inaccurate user who does not know ID Since the access to data itself is refused, while reading of inaccurate data is avoidable In the usual technical knowledge, even if access is successful with a certain means, since access to the cryptographic key written in the system area is impossible, it should not decode encryption data to raw data, but should devise a thoroughgoing security step in this point.

[0043] Drawing 6 is instantiation structural drawing of the data format containing ID information written in a system area, and a cryptographic key. In this drawing, the first example (a) has the magnitude of 20 bytes by all that consisted of each information on 8 bytes of ID information, 8 bytes of DES (Data Encryption Standard: U.S. federal government standard code specification) cryptographic key, 2 bytes of manufacture year, 1 byte of manufacture moon, and 1 byte of manufacture date. Moreover, the second example (b) has the magnitude of 36 bytes by all that consisted of each information on 8 bytes of ID information, 24 bytes of Triple DES cryptographic key, 2 bytes of manufacture year, 1 byte of manufacture moon, and 1 byte of manufacture date.

[0044] It is decided by whether the dependability of a cryptographic key is thought as important chiefly, or storage capacity pressure of a system area is avoided whether to adopt format [which]. In addition, the byte count of illustration, the class of cryptographic key, and format structure are instantiation to the last. What is necessary is just to, write the information (ID information) in which solid-state discernment of CD-R1 is possible, and the predetermined key information (cryptographic key) which can be decoded from encryption data to raw data while raw data is convertible for encryption data in the system area of CD-R1 in short.

[0045] Drawing 7 is the rough block block diagram of a write-once mold optical disk record regenerative apparatus (henceforth a "CD-R record regenerative apparatus").

The spindle motor 31 which this CD-R record regenerative apparatus 30 supports the clamping area (information non-recording area prepared among T1-T2 of drawing 1 (a)) of CD-R1, and carries out a rotation drive in the predetermined direction, The optical pickup 33 which spaces substrate 1b of CD-R1, and irradiates the object for record, or the laser 32 for playback (generally infrared laser with a wavelength of 770-830nm) at recording layer 1c, While having the coarse adjustment motor 34 made to move an optical pickup 33 to radial [of a disk] in harmony with the seeking motor which is not illustrated [which was prepared in the interior of an optical pickup 33] The disk roll control section 35 which controls the rotational speed of a spindle motor 31, The rotational speed of the coarse adjustment motor 34, and the coarse adjustment motor control section 36 which controls a hand of cut, The pickup control section 37 which performs control of the location of an optical pickup 33, or laser reinforcement, A synchronous wobbles signal and an ATIP wobbles signal are detected from the trace signal of 1f of guide rails of CD-R1. The wobbling control section 38 which reproduces at least ATIP information including the timing information for a disk roll control, or the information on a disk that a manufacturer can be specified, It has playback/record control section 39 which controls the reading signal from an optical pickup 33, conversion of waveform of the write-in signal to an optical pickup 33, etc., and has further the controller 40 which generalizes each of these control sections. This controller 40 is equivalent to an access means, a read-out means, a judgment means, and a write-in means given in the summary of invention.

[0046] the CD-R record regenerative apparatus 30 is built in the expansion slot of the host equipments 41, such as a personal computer, (or it carries out external -- having), connects between host equipment 41 and controllers 40 by cable 41a of predetermined signal specification (for example, SCSI:Small Computer System Interface), and is used.

[0047] The CD-R record regenerative apparatus 30 which has such a configuration can perform record and playback of recording information of the information on CD-R1 as it is shown below. in addition, CD-R1 -- CD-ROM -- although it is a compatible device and information playback of CD-ROM is also possible for the CD-R record regenerative apparatus 30, since there is no direct relation, explanation is abbreviated to this invention.

[0048] If the application program only for CD-R records (it abbreviates to "AP" below.) is executed with <record actuation of information on CD-R1> host equipment 41, the laser on-the-strength calibration command from AP will be first told to a controller 40. While a controller 40 answers this command, tells a necessary command

to each control section and locating an optical pickup 33 in an PCA sky field (field which is not tried, written and carried out) of CD-R1 After controlling rotational speed of a spindle motor 31 (it controls so that the relative velocity in the current position of an optical pickup 33 turns into a predetermined rate), the laser 32 for record of provisional reinforcement (Hazama's 5.5-8mW arbitration power) is irradiated from an optical pickup 33 to an PCA sky field, and trial writing is performed. Position control of an optical pickup 33 and rotational-speed control of a spindle motor 31 are performed according to the information (timing information and ATIP information) reproduced from the trace signal of 1f of guide rails of CD-R1.

[0049] Subsequently, a controller 40 reads the data written [were tried and] and set to PCA through playback/record control section 39, and returns the data to AP of host equipment 41. AP tries and writes, compares data with expected value, judges the propriety of laser reinforcement, and if a judgment result is "**" while carrying out increase and decrease of the laser reinforcement of accommodation and publishing a laser on-the-strength calibration command again, if a judgment result is "no", it will start record actuation of the information on CD-R1.

[0050] This record actuation transmitting the necessary record data chosen suitably to a controller 40 from AP, and performing the roll control of a spindle motor 31, and position control of an optical pickup 33 through each control section under control of this controller 40 by the user, while modulating the laser 32 for record from an optical pickup 33 by the above-mentioned record data, it records on the data area of CD-R1. And if record is completed, while closing all sessions and writing TOC of the session information in a lead-in groove (RI), lead-out (RO) is formed after the last session.

[0051] In case the recording information of <playback actuation of recording information of CD-R1> CD-R1 is reproduced, Above AP (application program only for CD-R records) is unnecessary. However, the driver software for performing the interconversion of the file system of CD-R1 and the file system of host equipment 41 is indispensable. By using the CD-R record regenerative apparatus 30 through this driver software, a user can access the file system of CD-R1, without being conscious of distinction with other storage devices, such as a hard disk with which host equipment 41 was equipped. That is, since the file structure recognized by the file system of an operating system is in sight of a user, a user can choose the file stored in other storage devices, and the file made into the purpose in CD-R1 in the same procedure, the file is copied, it can stick on other storage devices, or, in the case of execution files, such as an EXE format, the file concerned can be opened and performed.

[0052] While the CD-R record regenerative apparatus 30 reads the TOC information in a lead-in groove (RI) and provides the driver software of host equipment 41 with it on the occasion of this file access When the read-out command of a specific file is received from the driver software concerned While specifying the truck of a data area (UA) with which the data of the file concerned were written in with reference to the TOC information in a lead-in groove (RI) and locating an optical pickup 33 in the starting position of the truck Control the rotational speed of a spindle motor 31, irradiate the laser 13 for playback (the point that power is stopped by about 0.2mW is removed, and it is the same as the laser for record) from an optical pickup 33 at CD-R1, and the file data concerned is read. A series of actuation of transmitting the reading data to host equipment 41 is performed.

[0053] While the CD-R record regenerative apparatus 30 of the gestalt of this operation can write in information on CD-R1 as above, playback of the information written in CD-R1 can also be performed. Although this CD-R record regenerative apparatus 30 is an indispensable component when writing in information on CD-R1 in a user phase, it is a user phase and is a component needed also when reproducing information written in CD-R1. CD-R1 -- CD-ROM -- it is a compatible device, the CD-ROM regenerative apparatus is carried in most, such as a personal computer of these days, it is possible to perform information playback of CD-R1 using that CD-ROM regenerative apparatus, and since this CD-ROM regenerative apparatus cannot be accessed at ID information or the cryptographic key which were written in the system area of CD-R1, also when reproducing too information written in CD-R1, the CD-R record regenerative apparatus 30 is an indispensable component.

[0054] <Data write-in processing by user> drawing 8 is a flow chart which shows the data write-in actuation (henceforth "data write-in processing by the user") performed in a user phase. In this processing, a user receives data non-recorded CD-R1 in a commercial scene, sets that CD-R1 in the CD-R record regenerative apparatus 30, and records necessary user data on CD-R1 concerned. About this user data, an especially important point is in the point which is the secret data which permit playback only to a specific man, i.e., the data which require secrecy. When the data which require this kind of secrecy were conventionally recorded on CD-R, data were enciphered by the predetermined cryptographic key, it recorded on CD-R, and storages, such as a floppy disk which stored the decode key of the encryption data concerned together with that CD-R, were distributed. However, coincidence distribution of such multimedia has possibility, such as loss at a distribution place, when taking time and effort, and it has the fault that management is troublesome.

[0055] CD-R1 of the gestalt of this operation has the merit that management is made easy and it can cancel above-mentioned un-arranging, without losing at a distribution place, since encryption data and the decode key of the encryption data are stored and distributed to one storage.

[0056] In drawing 8 , if the data write-in processing by the user is started, the CD-R record regenerative apparatus 30 will judge the existence of the write-in instruction from host equipment 41 (step S31). And if there is a write-in instruction, the disk information of CD-R1 will be acquired (step S32). This disk information is the information that the manufacturer of CD-R1 concerned can be specified, for example, is starting position information on a lead-in groove (RI) included in ATIP information. It is because these starting position information differs for every manufacturer of a disk, so it is possible to deduce a manufacturer from this starting position information.

[0057] Acquisition of disk information judges [next] whether the disk information and a predetermined support list are collated, and the manufacturer of CD-R1 concerned is indicated by the support list (step S33). A support list is recorded on the nonvolatile memory (it is the rewritable nonvolatile memory of a flash memory etc. in order to enable renewal of a list preferably) prepared in the interior of a controller 40. When the manufacturer of CD-R1 concerned is not indicated by the support list After CD-R1 concerned records user data on the user area (UA) of CD-R1 concerned by the plaintext (raw data which are not enciphered) noting that it is a disk (non-supporting disk) which does not support the below-mentioned security mode (step S34), it ends processing. In addition, it is desirable to build download service of the above-mentioned support list. Such a distribution method is easily realizable by using the Internet techniques, such as for example, a WWW (Wold Wide Web) server and a FTP (File Transform Protocol) server.

[0058] On the other hand, when the manufacturer of CD-R1 concerned is indicated by the support list, CD-R1 concerned generates ID information and a cryptographic key first noting that it is a disk (support disk) which supports the below-mentioned security mode (step S35). ID information is acquired from an independent organization in exchange for a user's identity information, as mentioned above. Next, after enciphering user data using the cryptographic key (step S36), information, such as ID information, a cryptographic key, and a record date, is written in the system area of CD-R1 concerned (step S37), further, encryption data are written in the user area (UA) of CD-R1 concerned, and processing (step S38) is ended. In addition, in step S37, a format of information, such as ID information written in the system area of CD-R1, and a place cryptographic key, a record date, is as being shown in drawing 4 (a) or (b).

[0059] Drawing 9 is drawing showing the time run of the above "data write-in processing by the user", and the thing equivalent to the host equipment 41 above-mentioned [the personal computer 51 in drawing], the thing equivalent to the CD-R record regenerative apparatus 30 above-mentioned [the CD-R writer 52], and CD-R53 are equivalent to above-mentioned CD-R1.

[0060] In this drawing, while a user loads the CD-R writer 52 with CD-R53, he operates a personal computer 51 and publishes a necessary write-in instruction for the CD-R writer 52. The CD-R writer 52 answers this write-in instruction, the disk information of CD-R53 is acquired, the manufacturer information included in that disk information and a predetermined support list are collated, and it judges whether it is a support disk. And if it is not a support disk, actuation by normal mode is notified to a personal computer 51, a personal computer 51 will answer this notice, user data will be transmitted to the CD-R writer 52 by the plaintext, and the CD-R writer 52 will write the user data of the plaintext transmitted from the personal computer 51 in the user area (UA) of CD-R53.

[0061] As a result of, collating the manufacturer information included in disk information, and a predetermined support list on the other hand, when it is judged that it is a support disk The CD-R writer 52 notifies actuation with security mode to a personal computer 51, and a personal computer 51 answers this notice. While generating ID information (from the above-mentioned independent organization to for example, acquisition), and a cryptographic key, user data are enciphered using the cryptographic key, and these data (ID information, a cryptographic key, and encryption data) are transmitted to the CD-R writer 52. The CD-R writer 52 writes encryption data in the user area (UA) of CD-R53, and ends "data write-in processing by the user" of an above single string while it writes ID information and the cryptographic key which were transmitted from the personal computer 51 in the system area of CD-R53.

[0062] Therefore, while according to this "processing data write-in [by the user]" being able to write ID information and a cryptographic key in that system area and the user data enciphered by the cryptographic key concerned can be written in that user area only about CD-R with the manufacturer information indicated by the predetermined support list, the data writing of a plaintext can be performed about other CD-Rs, such as a no brand article.

[0063] Consequently, the user who wishes security nature will use positively a support disk (CD-R with the manufacturer information indicated by the support list), can forbid after all use of no brand CD-R which cannot deny existence of a crude article as a matter of fact, and can aim at dependability reservation of the data writing

of CD-R.

[0064] <Data regeneration by user> drawing 10 is a flow chart which shows the data playback actuation (henceforth "data regeneration by the user") performed in a user phase. In this processing, a user receives CD-R1 in which ID information, a cryptographic key, and encryption data were written by data write-in processing by the above-mentioned user, sets that CD-R1 in the CD-R record regenerative apparatus 30, reads a cryptographic key and encryption data from that CD-R1, and performs a series of processings in which encryption data are decoded using a cryptographic key. An especially important point is in this the processing of a series of for two kinds of users to exist. The first user is a user (henceforth a "registered user") who knows just ID information, and the second user is a user (henceforth an "inaccurate user") who does not know just ID information.

[0065] In drawing 10 , if the data regeneration by the user is started, the CD-R record regenerative apparatus 30 will judge the existence of the playback instruction from host equipment 41 (step S41). And if there is a playback instruction, ID input request is published to host equipment 41 (step S42), and ** will display predetermined GUI (Graphical User Interface) of **** for ID input on a screen, and host equipment 41 will receive ID input from the keyboard by the user etc. (step S43), and will transmit inputted ID information to the CD-R record regenerative apparatus 30.

[0066] The CD-R record regenerative apparatus 30 reads ID information currently written in the system area of CD-R1. Judge coincidence with ID information transmitted from host equipment 41 (step S44), and if inharmonious, while judging it as an inaccurate user and ending processing as it is, if it is coincidence, it will be judged as a registered user. The cryptographic key currently written in the system area of CD-R1 and the encryption data currently written in the data area are read, and it transmits to host equipment 41 (step S45). After host equipment 41 decodes encryption data using the cryptographic key and permits a registered user's access to the decode data concerned, it ends processing.

[0067] Drawing 11 is drawing showing the time run of the above "data regeneration by the user", and the thing equivalent to the host equipment 41 above-mentioned [the personal computer 51 in drawing], the thing equivalent to the CD-R record regenerative apparatus 30 above-mentioned [the CD-R writer 52], and CD-R53 are equivalent to above-mentioned CD-R1.

[0068] In this drawing, while a user loads the CD-R writer 52 with CD-R53, he operates a personal computer 51 and publishes a necessary playback instruction for the CD-R writer 52. The CD-R writer 52 answers this playback instruction, ID request

is returned to a personal computer 51, and, as for a personal computer 51, ** displays GUI of **** for ID input on a screen. A user inputs predetermined ID information (ID information justly notified from the distribution place of CD-R53) according to the GUI, and a personal computer 51 transmits inputted ID information to the CD-R writer 52.

[0069] A CD-R writer 52 reads the ID information currently written in the system area of CD-R53, judges coincidence with the ID information transmitted from the personal computer 51, if it is in agreement while it will be judged to be an inaccurate user, will stop processing and will refuse playback, if it is inharmonious, it will judge to be a registered user, it reads the cryptographic key currently written in the system area of CD-R53, and the encryption data currently written in the data area, and transmits them to a personal computer 51. After a personal computer 51 decodes encryption data using the cryptographic key and permits access from a registered user, it ends "data regeneration by the user" of an above single string.

[0070] Therefore, while a registered user and an inaccurate user are discriminable using ID information currently written in the system area of CD-R according to this "data regeneration by the user" Restrict, when data regeneration is performed by the registered user, and the cryptographic key written in the system area of CD-R and the encryption data written in the data area are transmitted to host equipment. Encryption data can be decoded with host equipment and accesses (for example, perusal thru/or activation, etc. of data) to the decoded raw data can be permitted.

[0071] consequently, an inaccurate user -- eliminating -- playback of data -- it can carry out -- unjust perusal, unjust activation, etc. of data -- preventing -- with -- **** -- the security nature of CD-R can be improved.

[0072] <Disk copy processing by user> drawing 12 is a flow chart which shows the disk copy actuation (henceforth "disk copy processing by the user") performed in a user phase. In this processing, a user by data write-in processing by the above-mentioned user CD-R1 in which ID information, a cryptographic key, and encryption data were written comes to hand, and the CD-R1 is set in the CD-R record regenerative apparatus 30. A cryptographic key and encryption data are read from the CD-R1, encryption data are decoded using the cryptographic key concerned, and a series of processings in which the decode data is written in intact CD-R set in another CD-R record regenerative apparatus 30 (it copies) are performed. Also in this the processing of a series of, two kinds of users of the inaccurate user who does not know just ID information with the registered user who knows just ID information exist.

[0073] In drawing 12 , if the disk copy processing by the user is started, the CD-R record regenerative apparatus (henceforth a "copied material CD-R record

regenerative apparatus") 10 loaded with CD-R1 of a copied material will judge the existence of the copy instruction from host equipment 41 (step S51). And if there is a copy instruction, ID input request is published to host equipment 41 (step S52), and ** will display predetermined GUI of **** for ID input on a screen, and host equipment 41 will receive ID input from the keyboard by the user etc. (step S53), and will transmit inputted ID information to the copied material CD-R record regenerative apparatus 30.

[0074] The copied material CD-R record regenerative apparatus 30 reads ID information currently written in the system area of CD-R1. Coincidence with ID information transmitted from host equipment 41 is judged (step S54). If inharmonious, while reading the encryption data which judged it as the inaccurate user and were written in the data area of CD-R1 and transmitting to host equipment 41 (step S55) If it is coincidence, the encryption data currently written in ID information, cryptographic key, and data area which judge it as a registered user and are written in the system area of CD-R1 will be read, and it will transmit to host equipment 41 (step S56).

[0075] Host equipment 41 judges whether ID information and a cryptographic key are contained in the transfer data. If ID information and a cryptographic key are contained, it is the CD-R record regenerative apparatus 30 (it is called below a "copy place CD-R record regenerative apparatus".) of a copy place one by one about the ID information and cryptographic key, and encryption data. It transmits to 10, or if ID information and a cryptographic key are not contained, transfer data (encryption data) itself is transmitted to the copy place CD-R record regenerative apparatus 30.

[0076] The copy place CD-R record regenerative apparatus 30 is the same procedure as the above-mentioned "data write-in processing by the user" (refer to drawing 8), when ID information and key information are included in the transmitted data. After recording the ID information and key information on CD-R of a copy place, encryption data are recorded on the data area of CD-R of a copy place. Or when ID information and key information are not included in the transmitted data, after recording encryption data on the data area of CD-R of a copy place, the completion of record is notified to host equipment 41, and a series of disk copy processings are ended.

[0077] Drawing 13 is drawing showing the time run of the above "disk copy processing by the user." The thing equivalent to the host equipment 41 above-mentioned [the personal computer 51 in drawing], That by which left-hand side CD-R53a is equivalent to CD-R1 of a copied material, the thing by which left-hand side CD-R writer 52a is equivalent to the above-mentioned copied material CD-R record regenerative apparatus 30, CD-R53b of the thing and right-hand side on which

right-hand side CD-R writer 52b is equivalent to the above-mentioned copy place CD-R record regenerative apparatus 30 is equivalent to CD-R of a copy place. That is, this example shows the example which carries out the disk copy of the recording information of left-hand side CD-R53a to right-hand side CD-R53b.

[0078] In this drawing, while a user loads the CD-R writers 52a and 52b with CD-Rs 53a and 53b of a copy place a copied material, respectively, he operates a personal computer 51 and publishes a necessary copy instruction to copied material CD-R writer 52a. Copied material CD-R writer 52a answers this copy instruction, and returns ID request to a personal computer 51, and, as for a personal computer 51, ** displays GUI of **** for ID input on a screen. A user inputs predetermined ID information (ID information justly notified from the distribution place of CD-R53a) according to the GUI, and a personal computer 51 transmits inputted ID information to copied material CD-R writer 52a.

[0079] Copied material CD-R writer 52a reads ID information currently written in the system area of CD-R53a, and coincidence with ID information transmitted from the personal computer 51 is judged. If inharmonious, while it is judged as an inaccurate user and the restrictive copy of only encryption data is permitted If in agreement, it will be judged as a registered user, and the encryption data currently written in ID information, cryptographic key, and data area which are written in the system area of CD-R53a are read, and it transmits to a personal computer 51.

[0080] A personal computer 51 transmits ID information, the cryptographic key, and encryption data which were read from CD-R53a of a copied material to copy place CD-R writer 52b while publishing a write-in instruction to copy place CD-R writer 52b. Copy place CD-R writer 52b writes the encryption data in the data area of CD-R53b, notifies the write-in completion to host equipment 41, and ends "disk copy processing by the user" of an above single string while it writes the ID information and cryptographic key in the system area of CD-R53b.

[0081] Therefore, while a registered user and an inaccurate user are discriminable using ID information currently written in the system area of copied material CD-R according to this "disk copy processing by the user" It restricts, when disk copy processing is performed by the registered user. The encryption data written in ID information, cryptographic key, and data area which were written in the system area of copied material CD-R can be transmitted to host equipment, and it can transmit to a copy place CD-R writer from host equipment, and can write in copy place CD-R (it copies).

[0082] Consequently, while a disk copy can be permitted only to a registered user and

the full duplicate object of copied material CD-R can be made to manufacture The restrictive copy of only encryption data can be permitted to an inaccurate user, can make the incomplete duplicate object (data cannot be used unless a code is decoded) which is not reusable manufacture substantially, and the appearance of unjust duplicate objects, such as a pirate edition CD, is prevented. Improvement in the security nature of CD-R can be aimed at.

[0083] As explained more than the <conclusion> CD-R1 of the gestalt of this operation It restricts, when writing in record data using a manufacturer's CD-R1 indicated by the support list. since the record data concerned were written in by the plaintext when record data were written in using a manufacturer's (or a manufacturer -- unknown) CD-R which is not indicated by the support list while enciphering and writing in the record data The user who is going to perform storage and distribution of the data which require secrecy The exceptional useful effectiveness that the trouble of the writing which will use a manufacturer's CD-R1 positively indicated by the above-mentioned support list with the natural thing, consequently prevents use of a no brand article, and originates in a crude article, or read-out is avoidable is acquired.

[0084] Moreover, since ID information is written in the system area of CD-R1 with a cryptographic key, in being able to perform user authentication in the case of subsequent data playback or a data copy and being able to permit data playback and a data copy only to a registered user using this ID information, even when copied to injustice, a follow-up survey can be performed from that ID information.

[0085] Moreover, that what is necessary is just to register a manufacturer's information into the above-mentioned support list, in order to do this merit so, while including the information that a manufacturer can be specified in the disk information of CD-R1 at the time of manufacture, since the existing information, such as lead-in groove starting position information on ATIP information, can be used for a manufacturer's specific information, there is also a merit on manufacture that it is not necessary to add a new process.

[0086] in addition, in the above explanation, although hiding information, such as ID information and a cryptographic key, is written in the system area, this system area may be the semantics of fields other than the field (typically data area) where direct access by the user was permitted, and you may be a lead-in groove not to mention above-mentioned PCA and PMA, and may be lead-out, or fields other than this exist -- you may be that field as long as it becomes.

[0087] Moreover, although explanation was not added especially about a cryptographic key, any of various cipher systems (for example, there are methods,

such as FEAL:Fast Encipherment Algorithm, besides the above-mentioned DES method.) which are generally known may be adopted. What is necessary is to take into consideration the difficulty of decode, the overhead of encryption processing or decode processing, the volume of encryption data, etc., and just to adopt a suitable method.

[0088] Moreover, the security function using ID information and the cryptographic key of said explanation The hardware property containing the microcomputer and the various peripheral devices which were chiefly mounted in the controller 40 of the CD-R record regenerative apparatus 30, or the main board of host equipment 41, Although organic association with software property, such as an operating system and various programs (driver software is included), realizes functionally Since hardware property and an operating system can use a general-purpose thing The indispensable matter indispensable for a security function in which ID information and the cryptographic key of said explanation were used Substantially, being together put by programs, such as the above-mentioned "data write-in processing by the user" (referring to drawing 8), "data regeneration by the user" (referring to drawing 10), or "disk copy processing by the user" (referring to drawing 12), can say.

[0089] Therefore, the security function using ID information concerning this invention or a cryptographic key includes the component (a unit article, a finished product, or semifinished product) containing record media or these record media, such as the floppy disk and optical disk which stored all those programs or its important section, a compact disk, a magnetic tape, a hard disk, or semiconductor memory. In addition, what the record medium or component has on a network not to mention that by which itself is in a distribution channel, and offers only the contents of record is contained.

[0090] Moreover, in the above explanation, although the example of CD-R was shown as a write-once mold optical disk, it does not restrict to this. For example, since DVD(Digital Video Disc or Digital Versatile Disc)-R can also perform one data writing, of course, he is the associate of a write-once mold optical disk. What is necessary is to read a CD-R record regenerative apparatus and a CD-R writer with a DVD-R record regenerative apparatus and a DVD-R writer, respectively, and just to replace them, while reading CD-R as DVD-R, when applying the above-mentioned explanation to DVD-R.

[0091]

[Effect of the Invention] According to invention according to claim 1, the information for security countermeasures is written in a part of the system area only about the write-once mold optical disk made by the predetermined manufacturer. Therefore, in

case the storage and distribution of data which require especially secrecy are performed, use of the write-once mold optical disk made by the predetermined manufacturer concerned can be forced.

[0092] Since the information for security countermeasures is written in the specific field (field for laser on-the-strength calibrations) to which the existence is disregarded at the time of playback of data according to invention according to claim 2, since the field concerned is widely understood as an object for laser on-the-strength calibrations also for about [that it is invisible] and this contractor to the user, it can secure invisibility also to this contractor that has this know how, and can maintain security.

[0093] According to invention according to claim 3, since the information for security countermeasures is written in the field to which direct access from a user is not permitted, all can make the information concerned the hiding information from a user.

[0094] According to invention according to claim 4, the security countermeasures based on solid-state discernment of a write-once mold optical disk can become possible, an illegal copy etc. can be prevented, and the security at the time of data playback can be improved.

[0095] According to invention according to claim 5, the user authentication using the information for security countermeasures can become possible, an inaccurate user can be eliminated using the authentication result, and the security at the time of data playback can be improved.

[0096] Since it is not exposed of raw data even when according to invention according to claim 6 the user data encryption using the information for security countermeasures should become possible and unjust authentication should be carried out, the secrecy nature of data is securable.

[0097] Even when according to invention according to claim 7 the decode using the information for security countermeasures of encryption data should be attained and unjust authentication should be carried out, unless the information for security countermeasures is read, it cannot be exposed of raw data and the secrecy nature of data can be secured.

[0098] According to invention according to claim 8, the information for security countermeasures is written in the system area only about the write-once mold optical disk made by the predetermined manufacturer. Therefore, in case the storage and distribution of data which require especially secrecy are performed, use of the write-once mold optical disk made by the predetermined manufacturer concerned can be forced.

[0099] According to invention according to claim 9, said access means, a read-out means, a judgment means, and a write-in means are realizable with organic association with the hardware property and this program containing a microcomputer.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the external view and its important section enlarged drawing of a write-once mold optical disk.

[Drawing 2] It is cross-section structural drawing of CD-R.

[Drawing 3] It is the mimetic diagram showing the guide rail (wobbles groove) formed in CD-R.

[Drawing 4] In order to form a guide rail in CD-R, it is the block diagram of a manufacturing installation used mainly in the manufacture phase of a disk.

[Drawing 5] It is the format conceptual diagram of each record section of CD-R.

[Drawing 6] It is instantiation structural drawing of the data format containing ID information written in a system area at the time of manufacture, and a cryptographic key.

[Drawing 7] It is the rough block block diagram of a write-once mold optical disk record regenerative apparatus.

[Drawing 8] It is the flow chart which shows the data write-in actuation (data write-in processing by the user) performed in a user phase.

[Drawing 9] It is drawing showing the time run of the data write-in processing by the

user.

[Drawing 10] It is the flow chart which shows the data playback actuation (data regeneration by the user) performed in a user phase.

[Drawing 11] It is drawing showing the time run of the data regeneration by the user.

[Drawing 12] It is the flow chart which shows the disk copy actuation (disk copy processing by the user) performed in a user phase.

[Drawing 13] It is drawing showing the time run of the disk copy processing by the user.

[Description of Notations]

PCA Power Calibration Area (a system area, field for laser on-the-strength calibrations)

PMA Program Memory Area (a system area, field for temporary storages of session information)

RI Lead-in groove (field for session information storing)

RO Lead-out (field for specifying the termination location of a user area)

UA User area (user area)

1 CD-R (Write-once Mold Optical Disk)

10 CD-R Record Regenerative Apparatus (Recording Device for Write-once Mold Optical Disks)

20 Controller (Access Means, Read-out Means, Judgment Means, Write-in Means)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－319329
（P2001－319329A）
(43)公開日　平成13年11月16日(2001.11.16)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ１１Ｂ　7/004		Ｇ１１Ｂ　7/004	Ｃ	５Ｄ０４４
7/007		7/007		５Ｄ０６６
19/02	５０１	19/02	５０１Ｊ	５Ｄ０９０
20/10		20/10	Ｈ	

審査請求　未請求　請求項の数９　ＯＬ　（全 18 頁）

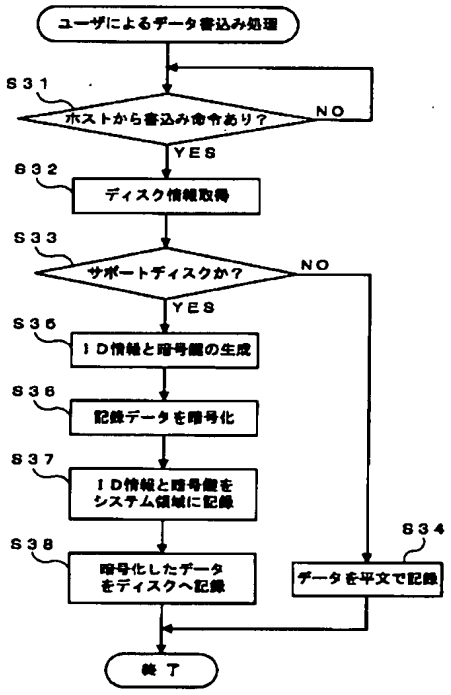
(21)出願番号　特願2000－138392(P2000－138392)
(22)出願日　平成12年５月11日(2000.5.11)

(71)出願人　000204284
太陽誘電株式会社
東京都台東区上野６丁目16番20号
(72)発明者　大村　幸秀
東京都台東区上野６丁目16番20号　太陽誘電株式会社内
(72)発明者　砂川　隆一
東京都台東区上野６丁目16番20号　太陽誘電株式会社内
(74)代理人　100096699
弁理士　鹿嶋　英實

最終頁に続く

(54)【発明の名称】　ライトワンス型光ディスク用記録装置および記録媒体

(57)【要約】
【課題】　所定の製造者のライトワンス型光ディスクを使用した場合にのみ、そのライトワンス型光ディスクにセキュリティ性を持たせ、それ以外のライトワンス型光ディスクとの差別化を図る。
【解決手段】　ユーザデータを書き込むためのユーザ領域と少なくとも当該書き込み動作を行う際にシステムによって利用されるシステム領域とを備えたライトワンス型光ディスク用の記録装置において、前記ライトワンス型光ディスクの製造者を調べて所定の製造者（によって作られたライトワンス型光ディスク：図８においては「サポートディスク」）である場合に、前記システム領域の一部にセキュリティ対策のための情報を書き込む。所定の製造者によって作られたライトワンス型光ディスクについてのみ、そのシステム領域の一部にセキュリティ対策のための情報が書き込まれる。



1

【特許請求の範囲】

【請求項１】　ユーザデータを書き込むためのユーザ領域と少なくとも当該書き込み動作を行う際にシステムによって利用されるシステム領域とを備えたライトワンス型光ディスク用の記録装置において、

前記ライトワンス型光ディスクの内部に電子的再生可能に記録された製造者情報を調べて所定の製造者情報である場合に、前記システム領域の一部にセキュリティ対策のための情報を書き込むようにしたことを特徴とするライトワンス型光ディスク用記録装置。

【請求項２】　前記システム領域は、ユーザデータを書き込む際のレーザ強度キャリブレーション用領域であることを特徴とする請求項１記載のライトワンス型光ディスク用記録装置。

【請求項３】　前記システム領域は、ユーザデータを書き込む際のセッション情報の一時格納用領域、または、ユーザ領域に書き込まれたユーザデータを再生する際に参照されるセッション情報格納用領域、若しくは、ユーザ領域の終了位置を明示するための領域のいずれかであることを特徴とする請求項１記載のライトワンス型光ディスク用記録装置。

【請求項４】　前記セキュリティ対策のための情報は、前記ライトワンス型光ディスクの固体識別のための識別情報であることを特徴とする請求項１記載のライトワンス型光ディスク用記録装置。

【請求項５】　前記セキュリティ対策のための情報は、ユーザ認証のための識別情報であることを特徴とする請求項１記載のライトワンス型光ディスク用記録装置。

【請求項６】　前記セキュリティ対策のための情報は、前記ユーザデータを暗号化するための鍵情報であることを特徴とする請求項１記載のライトワンス型光ディスク用記録装置。

【請求項７】　前記セキュリティ対策のための情報は、前記ユーザ領域に書き込まれた暗号化データを復号するための鍵情報であることを特徴とする請求項１記載のライトワンス型光ディスク用記録装置。

【請求項８】　ライトワンス型光ディスクにアクセスするアクセス手段と、

前記アクセス手段を介して前記ライトワンス型光ディスクから製造者情報を読み出す読み出し手段と、

前記アクセス手段によって読み出された製造者情報が所定の製造者情報であるか否かを判定する判定手段と、

前記判定手段の判定結果が否でない場合に前記ライトワンス型光ディスクのシステム領域にセキュリティ対策のための情報を書き込む書き込み手段と、

を備えたことを特徴とするライトワンス型光ディスク用記録装置。

【請求項９】　ライトワンス型光ディスクにアクセスするアクセス手段と、前記アクセス手段を介して前記ライトワンス型光ディスクから製造者情報を読み出す読み出し手段と、

前記アクセス手段によって読み出された製造者情報が所定の製造者情報であるか否かを判定する判定手段と、

前記判定手段の判定結果が否でない場合に前記ライトワンス型光ディスクのシステム領域にセキュリティ対策のための情報を書き込む書き込み手段とを実現するためのプログラムを格納したことを特徴とする記録媒体。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ライトワンス型光ディスク用記録装置および記録媒体に関する。詳しくは、１回だけデータを書き込むことができるＣＤ－Ｒ（Compact Disc Recordable）に代表されるライトワンス型光ディスクに適用する記録装置および記録媒体に関する。

【０００２】

【従来の技術】各種コンテンツやコンピュータプログラム等の電子データの配布媒体として、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）が多用されている。ＣＤ－ＲＯＭは、電子データを記録したマスタＣＤからプレス成型等によって製造される複製物であり、主に大量配布のメディアに用いられるが、配布数（製造数）の少ないサンプル版ＣＤやプライベートＣＤなどには、ライトワンス型の光ディスク装置、典型的にはＣＤ－Ｒが用いられる。ＣＤ－Ｒは透明なディスク基板と反射層（詳細な構造は後述する。）との間に有機色素からなる記録層を有している点でＣＤ－ＲＯＭと構造上の相違があり、専用の記録装置（ＣＤ－Ｒライター）を用いて当該記録層に高出力レーザを照射し、熱的反応によって当該記録層に情報ピットを形成することにより、ユーザ段階で情報の記録を行うことができるものである。

【０００３】ＣＤ－Ｒは上記のとおり情報の消去や上書きができない（追記は可能）ライトワンス型である。すなわち、一度書き込んだ情報の消去や書き換えが不可能である。したがって、不正者による情報の消去や改ざんを確実に防止できるという優れた利点を持つことから、特に保全を要する電子データの保管や配布などの用途に欠かせない記憶媒体となっている。

【０００４】

【発明が解決しようとする課題】（１）　しかしながら、従来のライトワンス型光ディスクにあっては、記録情報の消去や改ざんを防止できるという優れた利点があるものの、記録情報の読み出しが自由であるため、記録情報の不正読み出しや不正コピーを防止できないという不都合があった。このため、秘匿を要する情報を記録したＣＤ－Ｒの保管に際しては、厳格な管理規則を適用しなければならないが、このような管理規則の運用は相当困難で、多くの場合、規則の不徹底や馴れなどから安易な傾向に流れやすく、不心得な者によるＣＤ－Ｒの持ち出しや情報の読み出しを阻止できない結果、秘匿すべき

情報の外部流出ないしは不正にコピーされたＣＤ－Ｒの出現を回避できないという問題点があった。なお、かかる問題点は、ＣＤ－Ｒに限らず、可搬型の記憶デバイス一般にいえることであるが、ＣＤ－Ｒについては特に深刻である。ＣＤ－Ｒは、そのライトワンス型の特徴を活かして保全を要する電子データの配布や保管などに広く用いられている現実に加え、不要になったＣＤ－Ｒを物理的に破壊（例えば、意図的に傷をつけたり切断したりする）しない限り、用済み後もその記録情報の不正読み取りが可能であるからである。

【０００５】（２）　また、従来のライトワンス型光ディスク、例えば、ＣＤ－Ｒにあっては、記録層に高出力レーザを照射し、熱的反応による情報ピットを形成することによって、ユーザ段階で情報の記録を行うものであるが、まれに、情報ピットの形成に失敗（書き込み失敗）したり、あるいは、情報ピットを形成できたとしてもその形成が不十分で読み出しの際にエラーを発生したり（読み出し失敗）することがある。こうしたトラブルは、特にノーブランド品を用いた場合に経験することがある。一般にノーブランド品の製造者責任は不明確であり、正規品（製造者を明示したもの）に比べて品質の悪いＣＤ－Ｒの存在を否定できないからである。このような背景を考慮すると、理想的にはユーザに対して正規品の使用を推奨すべきであるが、実際にはノーブランド品は正規品に比べて安価に入手できることなどの理由から、ノーブランド品の利用者は結構多く、一部とはいえ粗悪品の存在に起因する上記トラブルの発生が問題となっている。

【０００６】したがって、本発明が解決しようとする課題は、所定の製造者のライトワンス型光ディスクを使用した場合にのみ、そのライトワンス型光ディスクにセキュリティ性を持たせることができ、以って、それ以外のライトワンス型光ディスクとの差別化を図ることにある。

【０００７】

【課題を解決するための手段】請求項１記載のライトワンス型光ディスク用記録装置は、ユーザデータを書き込むためのユーザ領域と少なくとも当該書き込み動作を行う際にシステムによって利用されるシステム領域とを備えたライトワンス型光ディスク用の記録装置において、前記ライトワンス型光ディスクの内部に電子的再生可能に記録された製造者情報を調べて所定の製造者情報である場合に、前記システム領域の一部にセキュリティ対策のための情報を書き込むようにしたことを特徴とする。これによれば、所定の製造者によって作られたライトワンス型光ディスクについてのみ、そのシステム領域の一部にセキュリティ対策のための情報が書き込まれる。

【０００８】請求項２記載のライトワンス型光ディスク用記録装置は、請求項１記載のライトワンス型光ディスク用記録装置において、前記システム領域は、ユーザデータを書き込む際のレーザ強度キャリブレーション用領域であることを特徴とする。これによれば、データの再生時にその存在が無視される特定の領域（レーザ強度キャリブレーション用領域）にセキュリティ対策のための情報が書き込まれる。

【０００９】請求項３記載のライトワンス型光ディスク用記録装置は、請求項１記載のライトワンス型光ディスク用記録装置において、前記システム領域は、ユーザデータを書き込む際のセッション情報の一時格納用領域、または、ユーザ領域に書き込まれたユーザデータを再生する際に参照されるセッション情報格納用領域、若しくは、ユーザ領域の終了位置を明示するための領域のいずれかであることを特徴とする。これによれば、いずれもユーザからの直接的なアクセスが許容されていない領域にセキュリティ対策のための情報が書き込まれる。

【００１０】請求項４記載のライトワンス型光ディスク用記録装置は、請求項１記載のライトワンス型光ディスク用記録装置において、前記セキュリティ対策のための情報は、前記ライトワンス型光ディスクの固体識別のための識別情報であることを特徴とする。これによれば、ライトワンス型光ディスクの固体識別に基づくセキュリティ対策が可能となる。

【００１１】請求項５記載のライトワンス型光ディスク用記録装置は、請求項１記載のライトワンス型光ディスク用記録装置において、前記セキュリティ対策のための情報は、ユーザ認証のための識別情報であることを特徴とする。これによれば、セキュリティ対策のための情報を利用したユーザ認証が可能となる。

【００１２】請求項６記載のライトワンス型光ディスク用記録装置は、請求項１記載のライトワンス型光ディスク用記録装置において、前記セキュリティ対策のための情報は、前記ユーザデータを暗号化するための鍵情報であることを特徴とする。これによれば、セキュリティ対策のための情報を利用したユーザデータの暗号化が可能となる。

【００１３】請求項７記載のライトワンス型光ディスク用記録装置は、請求項１記載のライトワンス型光ディスク用記録装置において、前記セキュリティ対策のための情報は、前記ユーザ領域に書き込まれた暗号化データを復号するための鍵情報であることを特徴とする。これによれば、セキュリティ対策のための情報を利用した暗号化データの復号が可能となる。

【００１４】請求項８記載のライトワンス型光ディスク用記録装置は、ライトワンス型光ディスクにアクセスするアクセス手段と、前記アクセス手段を介して前記ライトワンス型光ディスクから製造者情報を読み出す読み出し手段と、前記アクセス手段によって読み出された製造者情報が所定の製造者情報であるか否かを判定する判定手段と、前記判定手段の判定結果が否でない場合に前記ライトワンス型光ディスクのシステム領域にセキュリテ

ィ対策のための情報を書き込む書き込み手段と、を備えたことを特徴とする。これによれば、所定の製造者によって作られたライトワンス型光ディスクについてのみ、そのシステム領域にセキュリティ対策のための情報が書き込まれる。

【００１５】請求項９記載の記録媒体は、ライトワンス型光ディスクにアクセスするアクセス手段と、前記アクセス手段を介して前記ライトワンス型光ディスクから製造者情報を読み出す読み出し手段と、前記アクセス手段によって読み出された製造者情報が所定の製造者情報であるか否かを判定する判定手段と、前記判定手段の判定結果が否でない場合に前記ライトワンス型光ディスクのシステム領域にセキュリティ対策のための情報を書き込む書き込み手段とを実現するためのプログラムを格納したことを特徴とする。これによれば、マイクロコンピュータを含むハードウェア資産と該プログラムとの有機的結合によって前記アクセス手段、読み出し手段、判定手段および書き込み手段が実現される。

【００１６】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を詳細に説明する。なお、以下の説明における様々な細部の特定ないし実例および数値や文字列その他の記号の例示は、本発明の思想を明瞭にするための、あくまでも参考であって、それらのすべてまたは一部によって本発明の思想が限定されないことは明らかである。また、周知の手法、周知の手順、周知のアーキテクチャおよび周知の回路構成等（以下「周知事項」）についてはその細部にわたる説明を避けるが、これも説明を簡潔にするためであって、これら周知事項のすべてまたは一部を意図的に排除するものではない。かかる周知事項は本発明の出願時点で当業者の知り得るところであるので、以下の説明に当然含まれている。

【００１７】図１は、ライトワンス型光ディスク（以下「ＣＤ－Ｒ」という。）の外観図（ａ）およびその要部拡大図（ｂ）である。これらの図において、ＣＤ－Ｒ１は、直径１２ｃｍ（直径８ｃｍのものもある。以下、直径１２ｃｍのもので説明する。）のディスク状を有しており、ディスクの中心に直径１５ｍｍのセンターホール１ａが形成されている。ディスクの中心Ｔ０からセンタホール１ａの壁（ディスク内縁Ｔ１）までの距離は７．５ｍｍ、Ｔ０からディスク外縁Ｔ７までの距離は６０ｍｍであり、このＴ１～Ｔ７の間に同心状の複数の記録領域、すなわち、ディスクの内周側から順にＰＣＡ（Power Calibration Area）、ＰＭＡ（Program Memory Area）、リードイン（図では「ＲＩ」と略している。）、データエリア（図では「ＵＡ」と略している。）およびリードアウト（図では「ＲＯ」と略している。）の各領域が設けられている。

【００１８】各領域を概説すると、Ｔ２～Ｔ３に位置するＰＣＡは、ＣＤ－Ｒ１にデータを記録する際に行われるレーザ強度調整のための試し書き領域である。この試し書きは一般に１００回程度可能であり、少なくとも１回のデータ記録で１回分の領域を消費する。Ｔ３～Ｔ４に位置するＰＭＡは、ＣＤ－Ｒ１でまだクローズしていないセッションのトラックがあるとき、そのトラック番号と開始／終了位置を一時的に保存する領域である。Ｔ４～Ｔ５に位置するリードイン（ＲＩ）は、セッショントラックの先頭（ディスクの内周側）にある領域で、セッションのＴＯＣ（Table Of Contents：ＣＤに記録されているトラック数、開始位置およびデータ領域の合計の長さ）を保存する領域である。セッションをクローズすると、ＰＭＡに一時保存されていた情報がこのリードイン（ＲＩ）に書き込まれる。

【００１９】Ｔ５～Ｔ６に位置するデータエリア（ＵＡ）は、ユーザ段階で実際にデータが書き込まれる領域である。データの記録容量は最大約６８０Ｍバイト（直径８ｃｍのものは最大約１９０Ｍバイト）であり、この記憶容量は録音時間で表すと最大約７４分（直径８ｃｍのものは最大約２１分）になる。データエリア（ＵＡ）は、リードイン（ＲＩ）のすぐ後ろから連続する所定サイズ（２Ｋバイト）単位の論理ブロックで管理されるようになっており、各論理ブロックごとに０から最大約３３０００までのＬＢＮ（Logical Block Number）が割り当てられるようになっている。Ｔ６～Ｔ７に位置するリードアウト（ＲＯ）は、セッションの最後（ディスクの外周側）にある領域で、データエリア（ＵＡ）の最後に到達したことを示す領域である。

【００２０】これら各領域のディスク上の位置はＴ３を除いて規格化されている。すなわち、Ｔ２はＴ０から２２．５ｍｍ離れた位置、Ｔ４はＴ０から２３ｍｍ離れた位置、Ｔ５はＴ０から２５ｍｍ離れた位置、Ｔ６はＴ０から５８ｍｍ離れた位置となるように規定されている。なお、図ではディスク外縁とリードアウト（ＲＯ）の終了位置とを同一の符号（Ｔ７）で示しているが、これは図示の都合である。リードアウト（ＲＯ）の実際の終了位置はＴ０から５８．５ｍｍ離れた位置になる。以下、特に断りのない限り、Ｔ７はリードアウト（ＲＯ）の終了位置を表すものとする。ちなみに、リードアウト（ＲＯ）の開始と終了位置（Ｔ６およびＴ７）はＣＤ－Ｒ１に記録するデータの量に応じて変化する。上記の実際値（Ｔ６＝５８ｍｍ、Ｔ７＝５８．５ｍｍ）は記憶データ量を最大にしたときのものである。

【００２１】図２は、ＣＤ－Ｒ１の断面構造図である。ＣＤ－Ｒ１は、透明で耐熱性、耐湿性および成形性に優れ、且つ、所要の光学的特性（屈折率や複屈折など）を備えた材料（例えばプラスチック）からなる基板１ｂの上に、有機色素からなる記録層１ｃ、アルミニウムなどの金属材料からなる反射層１ｄおよび樹脂等の硬質材料からなる保護層１ｅを積層して形成されている。断面全体の厚さは１．２ｍｍである。

【００２２】ＣＤ－ＲＯＭとの構造上の相違は、記録層１ｃを有する点、および記録層１ｃと基板１ｂとの間にウォッブルグルーブと呼ばれる渦巻状の案内溝１ｆが形成されている点にある。ＣＤ－Ｒ１へのデータの記録は基板１ｂの裏側から案内溝１ｆに沿って記録用の強いレーザを照射し、記録層１ｃを加熱して情報ピット（pit：再生用のレーザ反射光を変調するための物理的変形変質部分）を形成することにより行われる。

【００２３】図３は、ＣＤ－Ｒ１の案内溝１ｆ（ウォッブルグルーブ）を示す模式図である。案内溝１ｆは同図（ａ）に示すように、ディスクの内周側から外周側（または外周側から内周側）に向かって一筆書きの要領で連続して形成されており、案内溝１ｆの幅は約０．５～０．７μｍ、間隔は約１．６μｍである。ユーザ段階におけるデータ記録は、案内溝１ｆに沿って、その案内溝１ｆ（または案内溝１ｆの間のランド部）直下の記録層１ｃに情報ピットを形成することによって行われる。なお、ＣＤ－Ｒ１の裏側から見て案内溝１ｆの凸部分をランド（山）、凹部分をグルーブ（谷）といい、一般に谷の部分をウォッブルグルーブというが、本明細書では山と谷を区別しない。

【００２４】ここで、案内溝１ｆの一の役割は、ユーザ段階のデータ記録時にディスクの回転速度を制御するためのタイミング情報を保持することにある。この役割のため、案内溝１ｆは、同図（ｂ）に示すように、所定の周期Ｔ１（例えばＴ１は２２．０５ｋＨｚに相当する周期）で蛇行（「ウォブリング」ともいう。）する形状に形成されている。データの記録時には、この蛇行を光ピックアップでトレースして周期Ｔ１を検出し、その検出周期Ｔ１が一定となるようにディスクの回転速度を制御することにより、データ記録時の光ピックアップとディスク間の相対速度を一定に保つ。

【００２５】案内溝１ｆの他の役割は、ディスク上の各記録領域（ＰＣＡ、ＰＭＡ、ＲＩ、ＵＡおよびＲＯ）の位置情報をはじめとした様々なディスク情報を保持することにある。ディスク情報はＡＴＩＰ（Absolute Time In Pregroove：通称「Ａチップ」という。）とも呼ばれており、ＡＴＩＰには、上記の位置情報のほかに、基準の記録レーザ強度やディスク回転速度、アプリケーションコードあるいはディスクタイプなどの各種情報が含まれると共に、さらに、ディスクの製造者を特定可能な情報（以下「製造者情報」という。）も含まれる。例えば、リードイン（ＲＩ）の開始位置情報はディスクの製造者ごとに異なるため、この開始位置情報を製造者情報として利用することができる。

【００２６】実際の案内溝１ｆは、例えば、同図（ｃ）に示すように、さらに細かく蛇行（または変形）しており、その細蛇行の周期Ｔ２によってＡＴＩＰ情報を多重化している。データの記録時にその周期（周波数）差を利用してタイミング情報とＡＴＩＰ情報を分離抽出し、タイミング情報を用いてディスクの回転制御を行うと共に、ＡＴＩＰ情報を用いてデータ記録位置等の制御を行うことが可能となる。

【００２７】なお、図示の例では、案内溝１ｆの細蛇行周期Ｔ２によってＡＴＩＰ情報の多重化を行っているが、この態様に限定されない。要は、データの記録時に案内溝１ｆをトレースしてそのトレース信号からＡＴＩＰ情報を再生できればよく、例えば、案内溝１ｆの側壁に凹凸等の物理的特異変形部分を形成し、その特異変形部分の間隔等からＡＴＩＰ情報を再生することも可能である。以下、説明の都合上、ＡＴＩＰ情報は上記の細蛇行周期Ｔ２によって多重化されているものとする。

【００２８】図４は、ＣＤ－Ｒ１に案内溝１ｆを形成するために、主としてディスクの製造段階で用いられる製造装置１０の構成図である。この図において、製造装置１０は、周期Ｔ１のタイミング情報に基づいて同期信号用ウォブリング信号（以下「同期ウォッブル信号」という。）を発生する第１ウォブリング信号発生回路１１と、少なくともディスクの製造者情報を含むＡＴＩＰ信号に基づいてＡＴＩＰウォッブル信号を発生する第２ウォブリング信号発生回路１２と、第１アンプ１３を介して同期ウォッブル信号を取り込み、この同期ウォッブル信号を用いて、不図示のレーザ光源から発射されたレーザ光を変調する第１光変調器１５と、第２アンプ１４を介してＡＴＩＰウォッブル信号を取り込み、このＡＴＩＰウォッブル信号を用いて、第１光変調器１５を通過したレーザ光を変調する第２光変調器１６と、第２光変調器１６を通過したレーザ光を反射するミラー１７と、ミラー１７で反射されたレーザ光を絞り込んでＣＤ－Ｒ１の記録面に照射する対物レンズ１８と、ＣＤ－Ｒ１を回転駆動するモータ１９とを備え、上記レーザ光の記録面への照射位置をＣＤ－Ｒ１の半径方向に移動させつつ、当該ＣＤ－Ｒ１を回転駆動することにより、図３（ａ）に示す渦巻き状の案内溝１ｆを形成する。

【００２９】ここで、第１光変調器１５を通過したレーザ光は同期ウォッブル信号による変調を受けており、さらに第２光変調器１６を通過したレーザ光はＡＴＩＰウォッブル信号による変調を受けている。すなわち、レーザ光は都合２回、変調されることとなる。したがって、ＣＤ－Ｒ１の記録面に形成される案内溝１ｆは、同期ウォッブル信号の周期Ｔ１とＡＴＩＰウォッブル信号の周期Ｔ２との合成周期に対応して“ウォブリング”（蛇行）することとなり、結局、図３（ｃ）に示すように、二つの周期（Ｔ１、Ｔ２）を有する合成蛇行形状が得られる。

【００３０】図５は、ＣＤ－Ｒ１の各記録領域のフォーマット概念図である。この図において、ＰＣＡ、ＰＭＡ、リードイン（ＲＩ）、データエリア（ＵＡ）およびリードアウト（ＲＯ）はそれぞれ、図１（ｂ）における同名部分に対応する。ＰＣＡおよびＰＭＡのサイズ（情

報書き込み可能容量）は特に決められていないが、前述の試し書き回数（一般に１００回程度）やセッション情報の一時記憶回数に見合った必要量、例えば、ＰＣＡで約３．５Ｍバイト程度、ＰＭＡで約２Ｍバイト程度の容量が確保されている。ちなみに、これらの例示容量からＰＣＡの開始位置（Ｔ２）とＰＭＡの開始位置（Ｔ３）は、規格化されたリードイン（ＲＩ）の開始位置（Ｔ４）を基準として、「Ｔ２＝Ｔ４－約３５秒」の位置、「Ｔ３＝Ｔ４－約１３秒」の位置と書き表すことができる。

【００３１】既述のとおり、ＰＣＡはデータ記録を行う際の試し書き領域、ＰＭＡはクローズされていないセッション情報を一時的に格納する領域であるから、これら二つの領域（ＰＣＡ／ＰＭＡ）はデータ記録時にのみ利用（アクセス）される領域である。一方、リードイン（ＲＩ）はクローズされたセッション情報をＴＯＣとして記録する領域、データエリア（ＵＡ）は実際にデータが書き込まれる領域、リードアウト（ＲＯ）はデータエリアの終わりを明示する領域であるから、これら三つの領域（リードイン／データエリア／リードアウト）はデータ記録時と再生時の両方で利用（アクセス）される領域である。

【００３２】他方、これらすべての領域をユーザからのアクセス容易性の点で見ると、すなわち、ＣＤ－Ｒ１の読み取り装置を備えたパーソナルコンピュータ等の利用者からその記憶内容を通常のツール（典型的には当該パーソナルコンピュータに搭載されたオペレーティングシステム上のファイルシステムなど）を用いて容易にアクセスできるか否かの点で評価すると、データエリア（ＵＡ）については当然ながらその記憶内容の全容把握は可能であるが、他の領域（ＰＣＡ、ＰＭＡ、リードインおよびリードアウト）の内容把握は不可能である。

【００３３】もちろん、特殊なツールを使用すれば可能ではあるが、そのようなツールは一般のユーザにとって入手困難であるため、かかる例外的なツールの利用を除けば、データエリア以外の他の領域（ＰＣＡ、ＰＭＡ、リードインおよびリードアウト）は、システムからのアクセスだけが許可された特殊な領域であるということができる。以下、この特殊領域のことを「システム領域」といい、ユーザからのアクセスが許可された領域のことを「ユーザ領域」ということにする。すなわち、データエリア（ＵＡ）はユーザ領域、それ以外のＰＣＡ、ＰＭＡ、リードイン（ＲＩ）およびリードアウト（ＲＯ）はシステム領域である。

【００３４】さて、本実施の形態におけるＣＤ－Ｒ１のポイントは、後述するように、①ユーザ段階でデータ記録を行う際にＣＤ－Ｒ１の製造者（ＣＤ－Ｒ１に書き込まれている製造者情報）を調べ、その製造者（製造者情報）が所定のサポートリストに記載されている場合に、当該ＣＤ－Ｒ１のシステム領域の一部にＣＤ－Ｒ１の固体識別情報（以下「ＩＤ情報」という。）と、所定の暗号鍵情報とを書き込むようにした点にある。②また、データ記録時に暗号鍵を用いて記録データを暗号化し、当該暗号化データを当該ＣＤ－Ｒ１に書き込むようにした点にある。③さらに、暗号化データを記録したＣＤ－Ｒ１のデータ再生やディスクコピーを行う際に、前記ＩＤ情報に基づくユーザ認証を行うようにした点にある。

【００３５】これらの①～③のポイントによって、秘匿を要するデータの管理や配布にセキュリティ性を持たせることができるようになる。すなわち、データを暗号化してＣＤ－Ｒ１に記録できる（②）とともに、この暗号化データを再生（復号）する際に、ＩＤ情報によるユーザ認証を行い（③）、正規ユーザ（ＩＤ情報を知っているユーザ）に対してのみデータ再生を許可することができるようになる。

【００３６】かかるセキュリティ機能は、ＣＤ－Ｒ１に最初から付加されているものではなく、ある条件を満たした場合に付加される機能である。すなわち、ＣＤ－Ｒ１の製造者が所定のサポートリストに記載されている場合にのみ（①）付加される限定的な機能であり、言い換えれば、サポートリストに記載されていない製造者（または製造者不明）のＣＤ－Ｒには付加されない機能であるから、この機能の有無によってＣＤ－Ｒの差別化を図ることができる。

【００３７】冒頭で説明したように、ユーザが市場で入手可能なＣＤ－Ｒ１は、製造者を明示した正規品とそれ以外の非正規品（ノーブランド品）とに分けられる。ノーブランド品は低価格であるものの粗悪品の存在を否定できないため、まれではあるが正常なデータ記録を行えないことがあった。特に重要なデータの管理や配布用途には正規品の使用を強制すべきであるが、そのような強制は実際上困難であるから、ノーブランド品の使用に伴うデータ書き込み失敗や読み出し失敗等のトラブルの可能性を否めなかった。

【００３８】本実施の形態におけるＣＤ－Ｒ１は、ユーザリストに記載された製造者のＣＤ－Ｒ１を使用することにより、ユーザは上記のセキュリティ機能を利用できるようになる。換言すれば、ユーザリストに記載されていないノーブランド品を使用した場合は上記のセキュリティ機能を利用できないから、特に秘匿を要するデータの保管や配布に適用する場合、ユーザは正規品を使用せざるを得なくなり、結果的にノーブランド品の使用を排除して、粗悪品に起因する記録データの書き込み失敗や読み出し失敗といったトラブルを回避することができるという格別のメリットが得られる。

【００３９】ＣＤ－Ｒ１のシステム領域に書き込むＩＤ情報はＣＤ－Ｒ１の全製造数にわたってユニークな値（重複しない値）を持つことが望ましいが、製造数が膨大になる場合、情報ビットが多ビット化してシステム領域の記憶容量を圧迫する懸念があるため、例えば、製造

ロットごとや製造ラインごとまたは製造時期ごとに異なる情報としてもよい。このＩＤ情報は、後述するように、データ再生やデータコピーを行う際のＣＤ－Ｒ１へのアクセス照合に用いられる。データの再生等を行うアプリケーションでＩＤの入力を要求し、入力されたＩＤとシステム領域に書き込まれているＩＤとの一致を判定して、一致の場合のみアクセスを許可する。これにより、不正なユーザ（ＩＤを知らないユーザ）によるデータの再生や複製を阻止し、データの流出や不正生成物の出現を回避することができる。

【００４０】ＩＤ情報の入手方法は、次の二つのものが考えられる。第一の方法はＩＤ情報を印刷した紙片をＣＤ－Ｒ１のパッケージに入れて一緒に出荷するというものである。ユーザはその紙片を見ながらＩＤ情報を入力する。この方法はパッケージソフトの分野で一般的に行われているインストール登録方法と類似しており、紙片を紛失しない限り、最も確実で簡単な方法である。なお、この方法の変形として、パッケージの表面やラベルにＩＤ情報を印刷したりすることもあるが、いずれもＣＤ－Ｒ１と一緒に適切なＩＤ情報をユーザに届けるという点で同一である。第二の方法はインターネット上の所定のＷｅｂサイトからＩＤ情報を入手するというものである。このＷｅｂサイトはあらゆるメーカ製のＣＤ－ＲについてユニークなｉＤ情報を発行できるように構成された動的Ｗｅｂサイトであり、ユーザからのＩＤ情報発行要求に応答して適切なＩＤ情報を当該ユーザ宛てに交付することができるものである。このようなＷｅｂサイトは、例えば、WWWサーバ上で動作するＡＳＰ（Active Server Pages）やＣＧＩ（Common Gateway Interface）等のサーバサイドスクリプトエンジンとデータベースとの組み合わせで構築することができる。この場合、ＣＤ－Ｒのパッケージには事前に登録用のコード情報（メーカ別またはその他の識別情報を示すコード情報）を印刷した紙片を入れておくことが望ましい。ユーザはこのコード情報を用いてＩＤ情報の交付を要求する。Ｗｅｂサイトは入力されたコード情報と交付済みＩＤ情報とをデータベースに登録して管理する。さらに第二の方法は次のように発展させることもできる。ユーザは初回のＩＤ情報発行要求時にそのユーザ専用のユーザ識別情報をＷｅｂサイトから受け取り、当該ユーザは以降のＩＤ情報発行要求時にそのユーザ識別情報を用いてＷｅｂサイトにアクセスする。このようにすると、Ｗｅｂサイトは交付済みＩＤ情報の履歴管理をユーザ識別情報ごと（すなわち、各ユーザごと）に行うことが可能となり、ユーザは過去に使用したＩＤ情報の履歴情報をＷｅｂサイトにアクセスしていつでも見ることができる。したがって、ユーザにとっては、自分で履歴管理をしなくてもよいというメリットが得られる。

【００４１】一方、システム領域に一緒に書き込まれる鍵情報は、ユーザ段階でデータエリアに書き込まれる生データを暗号化するために用いられる。すなわち、データの記録を行うアプリケーションで暗号鍵を読み出し、この暗号鍵を用いて生データを暗号化データに変換した後、その暗号化データをＣＤ－Ｒ１のデータエリアに書き込む。この暗号鍵は暗号化データを復号する際にも用いられる。すなわち、データの再生時に、データの再生を行うアプリケーションでＩＤの入力を要求し、入力されたＩＤとシステム領域に書き込まれているＩＤとの一致を判定して、一致の場合に暗号鍵と暗号化データを読み出し、その暗号鍵を用いて暗号化データを復号し、生データに変換してユーザの利用に供する。

【００４２】したがって、ＩＤを知らない不正なユーザは、データへのアクセス自体を拒否されるから、不正なデータの読み取りを回避できると共に、万が一、何らかの手段でアクセスが成功したとしても、システム領域に書き込まれた暗号鍵へのアクセスは通常の技術知識では不可能であるから、暗号化データを生データに復号することができず、この点において万全の保全策を講じることができる。

【００４３】図６は、システム領域に書き込まれるＩＤ情報と暗号鍵を含むデータフォーマットの例示構造図である。この図において、第一の例（ａ）は、８バイトのＩＤ情報、８バイトのＤＥＳ（Data Encryption Standard：アメリカ連邦政府標準暗号規格）暗号鍵、２バイトの製造年、１バイトの製造月および１バイトの製造日の各情報から構成された全部で２０バイトの大きさを有している。また、第二の例（ｂ）は、８バイトのＩＤ情報、２４バイトのトリプルＤＥＳ暗号鍵、２バイトの製造年、１バイトの製造月および１バイトの製造日の各情報から構成された全部で３６バイトの大きさを有している。

【００４４】いずれのフォーマットを採用するかは、もっぱら暗号鍵の信頼性を重視するか、または、システム領域の記憶容量圧迫を回避するかで決まる。なお、図示のバイト数や暗号鍵の種類およびフォーマット構造はあくまでも例示である。要はＣＤ－Ｒ１の固体識別が可能な情報（ＩＤ情報）と、生データを暗号化データに変換できると共に暗号化データから生データに復号できる所定のキー情報（暗号鍵）とをＣＤ－Ｒ１のシステム領域に書き込んでおけばよい。

【００４５】図７は、ライトワンス型光ディスク記録再生装置（以下「ＣＤ－Ｒ記録再生装置」という。）の概略的なブロック構成図である。このＣＤ－Ｒ記録再生装置３０は、ＣＤ－Ｒ１のクランピングエリア（図１（ａ）のＴ１～Ｔ２の間に設けられた情報非記録エリア）を担持して所定方向に回転駆動するスピンドルモータ３１と、ＣＤ－Ｒ１の基板１ｂを透して記録層１ｃに記録用または再生用のレーザ（一般に波長７７０～８３０ｎｍの赤外レーザ）３２を照射する光ピックアップ３３と、光ピックアップ３３の内部に設けられた不図示の

シークモータと協調して光ピックアップ３３をディスクの半径方向に移動させる粗動モータ３４とを備えると共に、スピンドルモータ３１の回転速度を制御するディスク回転制御部３５と、粗動モータ３４の回転速度と回転方向を制御する粗動モータ制御部３６と、光ピックアップ３３の位置やレーザ強度の制御を行うピックアップ制御部３７と、ＣＤ－Ｒ１の案内溝１ｆのトレース信号から同期ウォッブル信号やＡＴＩＰウォッブル信号を検出して、ディスク回転制御のためのタイミング情報や少なくともディスクの製造者を特定可能な情報を含むＡＴＩＰ情報を再生するウォブリング制御部３８と、光ピックアップ３３からの読み取り信号や光ピックアップ３３への書き込み信号の波形変換等の制御を行う再生／記録制御部３９とを備え、さらに、これらの各制御部を統括するコントローラ４０を備える。このコントローラ４０は、発明の要旨に記載のアクセス手段、読み出し手段、判定手段および書き込み手段に相当する。

【００４６】ＣＤ－Ｒ記録再生装置３０は、パーソナルコンピュータ等のホスト装置４１の拡張スロットに内蔵され（または外付けされ）、ホスト装置４１とコントローラ４０との間を所定の信号規格（例えば、ＳＣＳＩ：Small Computer System Interface）のケーブル４１ａで接続して用いられる。

【００４７】このような構成を有するＣＤ－Ｒ記録再生装置３０は、以下に示すとおり、ＣＤ－Ｒ１への情報の記録とその記録情報の再生を行うことができる。なお、ＣＤ－Ｒ１はＣＤ－ＲＯＭコンパチのデバイスであり、ＣＤ－Ｒ記録再生装置３０は、ＣＤ－ＲＯＭの情報再生も可能であるが、本発明とは直接の関連がないため説明を省略する。

【００４８】＜ＣＤ－Ｒ１への情報の記録動作＞ホスト装置４１でＣＤ－Ｒ記録専用アプリケーションプログラム（以下「ＡＰ」と省略する。）を実行すると、まず、ＡＰからのレーザ強度キャリブレーションコマンドがコントローラ４０に伝えられる。コントローラ４０はこのコマンドに応答して各制御部に所要の指令を伝え、光ピックアップ３３をＣＤ－Ｒ１のＰＣＡ空領域（試し書きされていない領域）に位置させると共に、スピンドルモータ３１の回転速度を制御（光ピックアップ３３の現在位置における相対速度が所定速度となるように制御）した後、光ピックアップ３３から暫定強度（５．５～８ｍＷの間の任意パワー）の記録用レーザ３２をＰＣＡ空領域に照射して試し書きを行う。光ピックアップ３３の位置制御およびスピンドルモータ３１の回転速度制御はＣＤ－Ｒ１の案内溝１ｆのトレース信号から再生された情報（タイミング情報およびＡＴＩＰ情報）に従って行われる。

【００４９】次いで、コントローラ４０は、再生／記録制御部３９を介してＰＣＡに試し書きされたデータを読み取り、そのデータをホスト装置４１のＡＰに返送する。ＡＰは、試し書きデータと期待値とを比較してレーザ強度の適否を判定し、判定結果が“否”であればレーザ強度を増減調節して再びレーザ強度キャリブレーションコマンドを発行する一方、判定結果が“適”であれば、ＣＤ－Ｒ１への情報の記録動作を開始する。

【００５０】この記録動作は、ユーザによって適宜に選択された所要の記録データをＡＰからコントローラ４０に伝え、このコントローラ４０の制御の下、各制御部を介してスピンドルモータ３１の回転制御および光ピックアップ３３の位置制御を行いつつ、上記記録データで光ピックアップ３３からの記録用レーザ３２を変調しながらＣＤ－Ｒ１のデータエリアに記録を行っていくというものである。そして、記録を完了すると、すべてのセッションを閉じ、そのセッション情報のＴＯＣをリードイン（ＲＩ）に書き込むと共に、最終セッションの後にリードアウト（ＲＯ）を形成する。

【００５１】＜ＣＤ－Ｒ１の記録情報の再生動作＞ＣＤ－Ｒ１の記録情報を再生する際に上記ＡＰ（ＣＤ－Ｒ記録専用アプリケーションプログラム）は不要である。但し、ＣＤ－Ｒ１のファイルシステムとホスト装置４１のファイルシステムとの相互変換を行うためのドライバソフトは必須である。ユーザはこのドライバソフトを介してＣＤ－Ｒ記録再生装置３０を利用することにより、ホスト装置４１に装備されたハードディスク等の他の記憶デバイスとの区別を意識せずにＣＤ－Ｒ１のファイルシステムにアクセスすることができる。すなわち、ユーザにはオペレーティングシステムのファイルシステムによって認識されたファイル構造が見えるから、ユーザは、他の記憶デバイスに格納されたファイルと同様の手順でＣＤ－Ｒ１内の目的とするファイルを選択し、そのファイルをコピーして他の記憶デバイスに貼り付けたり、またはＥＸＥ形式等の実行ファイルの場合は当該ファイルをオープンして実行したりすることができる。

【００５２】ＣＤ－Ｒ記録再生装置３０は、このファイルアクセスに際して、リードイン（ＲＩ）内のＴＯＣ情報を読み出してホスト装置４１のドライバソフトに提供すると共に、当該ドライバソフトから特定ファイルの読み出しコマンドを受け取った場合は、リードイン（ＲＩ）内のＴＯＣ情報を参照して当該ファイルのデータが書き込まれたデータエリア（ＵＡ）のトラックを特定し、そのトラックの開始位置に光ピックアップ３３を位置させると共に、スピンドルモータ３１の回転速度を制御し、光ピックアップ３３から再生用のレーザ（パワーが０．２ｍＷ程度に抑えられる点を除き記録用のレーザと同じもの）１３をＣＤ－Ｒ１に照射して当該ファイルデータを読み取り、その読み取りデータをホスト装置４１に転送するという一連の動作を実行する。

【００５３】以上のとおり、本実施の形態のＣＤ－Ｒ記録再生装置３０は、ＣＤ－Ｒ１への情報の書き込みを行うことができると共に、ＣＤ－Ｒ１に書き込まれた情報

の再生も行うことができる。このＣＤ－Ｒ記録再生装置３０は、ユーザ段階でＣＤ－Ｒ１への情報の書き込みを行う場合に必要不可欠な構成要素であるが、ユーザ段階で、ＣＤ－Ｒ１に書き込まれた情報の再生を行う場合も必要とされる構成要素である。ＣＤ－Ｒ１はＣＤ－ＲＯＭコンパチのデバイスで、昨今のパーソナルコンピュータ等のほとんどにはＣＤ－ＲＯＭ再生装置が搭載されており、そのＣＤ－ＲＯＭ再生装置を利用してＣＤ－Ｒ１の情報再生を行うことも可能であるが、このＣＤ－ＲＯＭ再生装置は、ＣＤ－Ｒ１のシステム領域に書き込まれたＩＤ情報や暗号鍵にアクセスできないから、やはり、ＣＤ－Ｒ１に書き込まれた情報の再生を行う場合もＣＤ－Ｒ記録再生装置３０は欠かせない構成要素である。

【００５４】＜ユーザによるデータ書き込み処理＞図８は、ユーザ段階で実行されるデータ書き込み動作（以下「ユーザによるデータ書き込み処理」という。）を示すフローチャートである。この処理では、ユーザは、データ未記録のＣＤ－Ｒ１を市場で入手し、そのＣＤ－Ｒ１をＣＤ－Ｒ記録再生装置３０にセットして、所要のユーザデータを当該ＣＤ－Ｒ１に記録する。このユーザデータについて、とりわけ重要な点は、特定の人に対してのみ再生を許可する非公開のデータ、すなわち、秘匿を要するデータである点にある。従来、この種の秘匿を要するデータをＣＤ－Ｒに記録する場合は、例えば、所定の暗号鍵でデータを暗号化してＣＤ－Ｒに記録し、そのＣＤ－Ｒと一緒に当該暗号化データの復号鍵を収めたフロッピィディスク等の記憶媒体を配布していた。しかし、このような複数媒体の同時配布は手間がかかる上、配布先での紛失等の可能性もあり、管理が面倒であるという欠点がある。

【００５５】本実施の形態のＣＤ－Ｒ１は、一つの記憶媒体に暗号化データと、その暗号化データの復号鍵とを収めて配布するので、配布先で紛失することもなく、管理を容易にして上記不都合を解消できるというメリットがある。

【００５６】図８において、ユーザによるデータ書き込み処理を開始すると、ＣＤ－Ｒ記録再生装置３０は、ホスト装置４１からの書き込み命令の有無を判定する（ステップＳ３１）。そして、書き込み命令があると、ＣＤ－Ｒ１のディスク情報を取得する（ステップＳ３２）。このディスク情報は当該ＣＤ－Ｒ１の製造者を特定可能な情報であり、例えば、ＡＴＩＰ情報に含まれる、リードイン（Ｒｉ）の開始位置情報である。この開始位置情報はディスクの製造者ごとに異なるため、この開始位置情報から製造者を割り出すことが可能であるからである。

【００５７】ディスク情報を取得すると、次に、そのディスク情報と所定のサポートリストとを照合して、当該ＣＤ－Ｒ１の製造者がサポートリストに記載されているか否かを判定する（ステップＳ３３）。サポートリストは、例えば、コントローラ４０の内部に設けられた不揮発性メモリ（好ましくはリストの更新を可能にするためフラッシュメモリ等の書き換え可能な不揮発性メモリ）に記録されたものであり、当該ＣＤ－Ｒ１の製造者がサポートリストに記載されていない場合は、当該ＣＤ－Ｒ１は後述のセキュリティモードをサポートしないディスク（非サポートディスク）であるとして、ユーザデータを平文（暗号化されない生のデータ）で当該ＣＤ－Ｒ１のユーザエリア（ＵＡ）に記録（ステップＳ３４）した後、処理を終了する。なお、上記サポートリストのダウンロードサービスを構築しておくことが望ましい。このような配布方式は、例えば、WWW（Wold Wide Web）サーバやＦＴＰ（File Transform Protocol）サーバ等のインターネット技術を用いることによって容易に実現することができる。

【００５８】一方、当該ＣＤ－Ｒ１の製造者がサポートリストに記載されている場合は、当該ＣＤ－Ｒ１は後述のセキュリティモードをサポートするディスク（サポートディスク）であるとして、まず、ＩＤ情報と暗号鍵を生成する（ステップＳ３５）。ＩＤ情報は、前述したように、例えば、ユーザの身元情報と引き換えに第三者機関から取得したものである。次に、その暗号鍵を用いてユーザデータを暗号化（ステップＳ３６）した後、ＩＤ情報および暗号鍵ならびに記録日付等の情報を当該ＣＤ－Ｒ１のシステム領域に書き込み（ステップＳ３７）、さらに、暗号化データを当該ＣＤ－Ｒ１のユーザエリア（ＵＡ）に書き込んで（ステップＳ３８）処理を終了する。なお、ステップＳ３７において、ＣＤ－Ｒ１のシステム領域に書き込むＩＤ情報や所暗号鍵ならびに記録日付等の情報のフォーマットは、図４（ａ）または（ｂ）に示すとおりである。

【００５９】図９は、上記「ユーザによるデータ書き込み処理」のタイムランを示す図であり、図中のパーソナルコンピュータ５１は上述のホスト装置４１に相当するもの、ＣＤ－Ｒライター５２は上述のＣＤ－Ｒ記録再生装置３０に相当するもの、ＣＤ－Ｒ５３は上述のＣＤ－Ｒ１に相当するものである。

【００６０】この図において、ユーザは、ＣＤ－Ｒ５３をＣＤ－Ｒライター５２に装填すると共に、パーソナルコンピュータ５１を操作して所要の書き込み命令をＣＤ－Ｒライター５２に発行する。ＣＤ－Ｒライター５２はこの書き込み命令に応答して、ＣＤ－Ｒ５３のディスク情報を取得し、そのディスク情報に含まれる製造者情報と所定のサポートリストとを照合してサポートディスクであるか否かを判定する。そして、サポートディスクでなければ、パーソナルコンピュータ５１にノーマルモードでの動作を通知し、パーソナルコンピュータ５１はこの通知に応答してユーザデータを平文でＣＤ－Ｒライター５２に転送し、ＣＤ－Ｒライター５２はパーソナルコンピュータ５１から転送された平文のユーザデータをＣ

Ｄ－Ｒ５３のユーザエリア（ＵＡ）に書き込む。

【００６１】一方、ディスク情報に含まれる製造者情報と所定のサポートリストとを照合した結果、サポートディスクであることを判定した場合は、ＣＤ－Ｒライター５２はパーソナルコンピュータ５１に対してセキュリティモードでの動作を通知し、パーソナルコンピュータ５１はこの通知に応答して、ＩＤ情報（例えば、前述の第三者機関から取得）と暗号鍵を生成すると共に、その暗号鍵を用いてユーザデータを暗号化し、これらのデータ（ＩＤ情報、暗号鍵および暗号化データ）をＣＤ－Ｒライター５２に転送する。ＣＤ－Ｒライター５２はパーソナルコンピュータ５１から転送されたＩＤ情報と暗号鍵をＣＤ－Ｒ５３のシステム領域に書き込むと共に、暗号化データをＣＤ－Ｒ５３のユーザエリア（ＵＡ）に書き込み、以上一連の「ユーザによるデータ書き込み処理」を終了する。

【００６２】したがって、この「ユーザによるデータ書き込み処理」によれば、所定のサポートリストに記載された製造者情報をもつＣＤ－Ｒについてのみ、そのシステム領域にＩＤ情報と暗号鍵を書き込むことができると共に、そのユーザエリアに当該暗号鍵で暗号化したユーザデータを書き込むことができる一方、ノーブランド品等の他のＣＤ－Ｒについては、平文のデータ書き込みを行うことができる。

【００６３】その結果、セキュリティ性を希望するユーザは、積極的にサポートディスク（サポートリストに記載された製造者情報をもつＣＤ－Ｒ）を使用することとなり、結局、粗悪品の存在を否定できないノーブランドＣＤ－Ｒの使用を事実上禁止して、ＣＤ－Ｒのデータ書き込みの信頼性確保を図ることができる。

【００６４】＜ユーザによるデータ再生処理＞図１０は、ユーザ段階で実行されるデータ再生動作（以下「ユーザによるデータ再生処理」という。）を示すフローチャートである。この処理では、ユーザは、前述のユーザによるデータ書き込み処理によって、ＩＤ情報および暗号鍵ならびに暗号化データが書き込まれたＣＤ－Ｒ１を入手し、そのＣＤ－Ｒ１をＣＤ－Ｒ記録再生装置３０にセットして、そのＣＤ－Ｒ１から暗号鍵と暗号化データを読み出し、暗号鍵を用いて暗号化データを復号するという一連の処理を実行する。この一連の処理において、とりわけ重要な点は、二種類のユーザが存在することにある。第一のユーザは正当なＩＤ情報を知っているユーザ（以下「正規ユーザ」という。）であり、第二のユーザは正当なＩＤ情報を知らないユーザ（以下「不正ユーザ」という。）である。

【００６５】図１０において、ユーザによるデータ再生処理を開始すると、ＣＤ－Ｒ記録再生装置３０は、ホスト装置４１からの再生命令の有無を判定する（ステップＳ４１）。そして、再生命令があると、ホスト装置４１に対してＩＤ入力要求を発行し（ステップＳ４２）、ホスト装置４１は、画面上にＩＤ入力を促がす旨の所定のＧＵＩ（Graphical User Interface）を表示してユーザによるキーボード等からのＩＤ入力を受け付け（ステップＳ４３）、入力されたＩＤ情報をＣＤ－Ｒ記録再生装置３０に転送する。

【００６６】ＣＤ－Ｒ記録再生装置３０は、ＣＤ－Ｒ１のシステム領域に書き込まれているＩＤ情報を読み出して、ホスト装置４１から転送されたＩＤ情報との一致を判定し（ステップＳ４４）、不一致であれば不正ユーザと判断してそのまま処理を終了する一方、一致であれば正規ユーザと判断して、ＣＤ－Ｒ１のシステム領域に書き込まれている暗号鍵とデータエリアに書き込まれている暗号化データとを読み出してホスト装置４１に転送する（ステップＳ４５）。ホスト装置４１は、その暗号鍵を用いて暗号化データを復号し、当該復号データに対する正規ユーザのアクセスを許容した後、処理を終了する。

【００６７】図１１は、上記「ユーザによるデータ再生処理」のタイムランを示す図であり、図中のパーソナルコンピュータ５１は上述のホスト装置４１に相当するもの、ＣＤ－Ｒライター５２は上述のＣＤ－Ｒ記録再生装置３０に相当するもの、ＣＤ－Ｒ５３は上述のＣＤ－Ｒ１に相当するものである。

【００６８】この図において、ユーザは、ＣＤ－Ｒ５３をＣＤ－Ｒライター５２に装填すると共に、パーソナルコンピュータ５１を操作して所要の再生命令をＣＤ－Ｒライター５２に発行する。ＣＤ－Ｒライター５２はこの再生命令に応答してＩＤ要求をパーソナルコンピュータ５１に返し、パーソナルコンピュータ５１は画面上にＩＤ入力を促がす旨のＧＵＩを表示する。ユーザは、そのＧＵＩに従って所定のＩＤ情報（ＣＤ－Ｒ５３の配布先から正当に通知されたＩＤ情報）を入力し、パーソナルコンピュータ５１は入力されたＩＤ情報をＣＤ－Ｒライター５２に転送する。

【００６９】ＣＤ－Ｒライター５２は、ＣＤ－Ｒ５３のシステム領域に書き込まれているＩＤ情報を読み出し、パーソナルコンピュータ５１から転送されたＩＤ情報との一致を判定して、不一致であれば不正ユーザと判断し、処理を中止して再生を拒否する一方、一致していれば正規ユーザと判断し、ＣＤ－Ｒ５３のシステム領域に書き込まれている暗号鍵とデータエリアに書き込まれている暗号化データとを読み出してパーソナルコンピュータ５１に転送する。パーソナルコンピュータ５１は、その暗号鍵を用いて暗号化データを復号し、正規ユーザからのアクセスを許容した後、以上一連の「ユーザによるデータ再生処理」を終了する。

【００７０】したがって、この「ユーザによるデータ再生処理」によれば、ＣＤ－Ｒのシステム領域に書き込まれているＩＤ情報を用いて正規ユーザと不正ユーザとを識別することができると共に、正規ユーザによってデー

タ再生処理が行われている場合に限り、ＣＤ－Ｒのシステム領域に書き込まれた暗号鍵とデータエリアに書き込まれた暗号化データとをホスト装置に転送し、ホスト装置で暗号化データの復号を行い、復号された生データへのアクセス（例えば、データの閲覧ないし実行等）を許容することができる。

【００７１】その結果、不正ユーザを排除してデータの再生を行うことができ、データの不正閲覧および不正実行等を防止し、以って、ＣＤ－Ｒのセキュリティ性を向上することができる。

【００７２】＜ユーザによるディスクコピー処理＞図１２は、ユーザ段階で実行されるディスクコピー動作（以下「ユーザによるディスクコピー処理」という。）を示すフローチャートである。この処理では、ユーザは、前述のユーザによるデータ書き込み処理によって、ＩＤ情報および暗号鍵ならびに暗号化データが書き込まれたＣＤ－Ｒ１を入手し、そのＣＤ－Ｒ１をＣＤ－Ｒ記録再生装置３０にセットして、そのＣＤ－Ｒ１から暗号鍵と暗号化データを読み出し、当該暗号鍵を用いて暗号化データを復号し、その復号データを別のＣＤ－Ｒ記録再生装置３０にセットされた未使用のＣＤ－Ｒに書き込む（コピーする）という一連の処理を実行する。この一連の処理においても、正当なＩＤ情報を知っている正規ユーザと正当なＩＤ情報を知らない不正ユーザの二種類のユーザが存在する。

【００７３】図１２において、ユーザによるディスクコピー処理を開始すると、コピー元のＣＤ－Ｒ１を装填したＣＤ－Ｒ記録再生装置（以下「コピー元ＣＤ－Ｒ記録再生装置」という。）１０は、ホスト装置４１からのコピー命令の有無を判定する（ステップＳ５１）。そして、コピー命令があると、ホスト装置４１に対してＩＤ入力要求を発行し（ステップＳ５２）、ホスト装置４１は、画面上にＩＤ入力を促がす旨の所定のＧＵＩを表示してユーザによるキーボード等からのＩＤ入力を受け付け（ステップＳ５３）、入力されたＩＤ情報をコピー元ＣＤ－Ｒ記録再生装置３０に転送する。

【００７４】コピー元ＣＤ－Ｒ記録再生装置３０は、ＣＤ－Ｒ１のシステム領域に書き込まれているＩＤ情報を読み出して、ホスト装置４１から転送されたＩＤ情報との一致を判定し（ステップＳ５４）、不一致であれば不正ユーザと判断してＣＤ－Ｒ１のデータエリアに書き込まれた暗号化データを読み出してホスト装置４１に転送（ステップＳ５５）する一方、一致であれば正規ユーザと判断してＣＤ－Ｒ１のシステム領域に書き込まれているＩＤ情報と暗号鍵およびデータエリアに書き込まれている暗号化データを読み出してホスト装置４１に転送する（ステップＳ５６）。

【００７５】ホスト装置４１は、その転送データにＩＤ情報と暗号鍵が含まれているか否かを判定し、ＩＤ情報と暗号鍵が含まれていればそのＩＤ情報と暗号鍵および暗号化データを順次にコピー先のＣＤ－Ｒ記録再生装置３０（以下「コピー先ＣＤ－Ｒ記録再生装置」という。）１０に転送し、または、ＩＤ情報と暗号鍵が含まれていなければ転送データ（暗号化データ）それ自体をコピー先ＣＤ－Ｒ記録再生装置３０に転送する。

【００７６】コピー先ＣＤ－Ｒ記録再生装置３０は、転送されたデータにＩＤ情報と鍵情報が含まれている場合、前述の「ユーザによるデータ書き込み処理」（図８参照）と同様の手順で、そのＩＤ情報と鍵情報をコピー先のＣＤ－Ｒに記録した後、暗号化データをコピー先のＣＤ－Ｒのデータエリアに記録し、または、転送されたデータにＩＤ情報と鍵情報が含まれていない場合は、暗号化データをコピー先のＣＤ－Ｒのデータエリアに記録した後、記録完了をホスト装置４１に通知して一連のディスクコピー処理を終了する。

【００７７】図１３は、上記「ユーザによるディスクコピー処理」のタイムランを示す図であり、図中のパーソナルコンピュータ５１は上述のホスト装置４１に相当するもの、左側のＣＤ－Ｒ５３ａはコピー元のＣＤ－Ｒ１に相当するもの、左側のＣＤ－Ｒライター５２ａは上述のコピー元ＣＤ－Ｒ記録再生装置３０に相当するもの、右側のＣＤ－Ｒライター５２ｂは上述のコピー先ＣＤ－Ｒ記録再生装置３０に相当するもの、右側のＣＤ－Ｒ５３ｂはコピー先のＣＤ－Ｒに相当するものである。すなわち、この例では、左側のＣＤ－Ｒ５３ａの記録情報を右側のＣＤ－Ｒ５３ｂにディスクコピーする例を示している。

【００７８】この図において、ユーザは、コピー元とコピー先のＣＤ－Ｒ５３ａ、５３ｂをそれぞれＣＤ－Ｒライター５２ａ、５２ｂに装填すると共に、パーソナルコンピュータ５１を操作して所要のコピー命令をコピー元ＣＤ－Ｒライター５２ａに発行する。コピー元ＣＤ－Ｒライター５２ａはこのコピー命令に応答してＩＤ要求をパーソナルコンピュータ５１に返し、パーソナルコンピュータ５１は画面上にＩＤ入力を促がす旨のＧＵＩを表示する。ユーザは、そのＧＵＩに従って所定のＩＤ情報（ＣＤ－Ｒ５３ａの配布先から正当に通知されたＩＤ情報）を入力し、パーソナルコンピュータ５１は入力されたＩＤ情報をコピー元ＣＤ－Ｒライター５２ａに転送する。

【００７９】コピー元ＣＤ－Ｒライター５２ａは、ＣＤ－Ｒ５３ａのシステム領域に書き込まれているＩＤ情報を読み出し、パーソナルコンピュータ５１から転送されたＩＤ情報との一致を判定して、不一致であれば不正ユーザと判断し、暗号化データのみの限定的コピーを許容する一方、一致していれば正規ユーザと判断し、ＣＤ－Ｒ５３ａのシステム領域に書き込まれているＩＤ情報と暗号鍵およびデータエリアに書き込まれている暗号化データを読み出してパーソナルコンピュータ５１に転送する。

【００８０】パーソナルコンピュータ５１は、コピー先ＣＤ－Ｒライター５２ｂに書き込み命令を発行すると共に、コピー元のＣＤ－Ｒ５３ａから読み出したＩＤ情報、暗号鍵および暗号化データをコピー先ＣＤ－Ｒライター５２ｂに転送する。コピー先ＣＤ－Ｒライター５２ｂはそのＩＤ情報と暗号鍵をＣＤ－Ｒ５３ｂのシステム領域に書き込むと共に、その暗号化データをＣＤ－Ｒ５３ｂのデータエリアに書き込み、その書き込み完了をホスト装置４１に通知して、以上一連の「ユーザによるディスクコピー処理」を終了する。

【００８１】したがって、この「ユーザによるディスクコピー処理」によれば、コピー元ＣＤ－Ｒのシステム領域に書き込まれているＩＤ情報を用いて正規ユーザと不正ユーザとを識別することができると共に、正規ユーザによってディスクコピー処理が行われている場合に限り、コピー元ＣＤ－Ｒのシステム領域に書き込まれたＩＤ情報と暗号鍵およびデータエリアに書き込まれた暗号化データをホスト装置に転送し、ホスト装置からコピー先ＣＤ－Ｒライターに転送して、コピー先ＣＤ－Ｒに書き込む（コピーする）ことができる。

【００８２】その結果、正規ユーザだけにディスクコピーを許可してコピー元ＣＤ－Ｒの完全複製物を製造させることができる一方、不正ユーザに対しては暗号化データのみの限定的コピーを許可し、実質的に再利用不能（暗号を解読しない限りデータを利用できない）な未完成複製物を製造させることができ、海賊版ＣＤ等の不正複製物の出現を防止して、ＣＤ－Ｒのセキュリティ性の向上を図ることができる。

【００８３】＜まとめ＞以上、説明したとおり、本実施の形態のＣＤ－Ｒ１は、サポートリストに記載された製造者のＣＤ－Ｒ１を使用して記録データの書き込みを行う場合に限り、その記録データを暗号化して書き込む一方、サポートリストに記載されていない製造者（または製造者不明）のＣＤ－Ｒを使用して記録データの書き込みを行う場合は当該記録データを平文で書き込むようにしたから、秘匿を要するデータの保管や配布を行おうとするユーザは、当然のことながら積極的に上記サポートリストに記載された製造者のＣＤ－Ｒ１を使用することとなり、その結果、ノーブランド品の使用を阻止して粗悪品に起因する書き込みや読み出しのトラブルを回避することができるという格別有益な効果が得られる。

【００８４】また、ＣＤ－Ｒ１のシステム領域に、暗号鍵と共にＩＤ情報を書き込むため、このＩＤ情報を用いて、事後のデータ再生やデータコピーの際のユーザ認証を行うことができ、正規ユーザに対してのみデータ再生やデータコピーを許容することができるうえ、万が一不正にコピーされた場合でも、そのＩＤ情報から追跡調査を行うことができる。

【００８５】また、かかるメリットを奏するためには製造時に、ＣＤ－Ｒ１のディスク情報に製造者を特定可能な情報を含めるとともに、上記のサポートリストに製造者の情報を登録するだけでよく、しかも、ＡＴＩＰ情報のリードイン開始位置情報などの既存情報を製造者の特定情報に利用できるから、新たな工程を追加する必要もないという製造上のメリットもある。

【００８６】なお、以上の説明では、ＩＤ情報や暗号鍵などの隠し情報をシステム領域に書き込んでいるが、このシステム領域とは、ユーザによる直接的なアクセスが許容された領域（典型的にはデータエリア）以外の領域という意味であり、前述のＰＣＡやＰＭＡはもちろんのこと、リードインであってもよいし、リードアウトであってもよく、あるいは、これ以外の領域が存在するならば、その領域であってもよい。

【００８７】また、暗号鍵については、特に説明を加えなかったが、一般的に知られている様々な暗号化方式（例えば、前述のＤＥＳ方式以外にも、ＦＥＡＬ：Fast Encipherment Algorithmなどの方式がある。）のいずれを採用してもかまわない。解読の困難性、暗号化処理や復号処理のオーバヘッドおよび暗号化データのボリューム等を勘案して適切な方式を採用すればよい。

【００８８】また、前記説明のＩＤ情報や暗号鍵を利用したセキュリティ機能は、もっぱらＣＤ－Ｒ記録再生装置３０のコントローラ４０やホスト装置４１のメインボードに実装されたマイクロコンピュータならびに各種周辺機器を含むハードウェア資産と、オペレーティングシステムや各種プログラム（ドライバソフトを含む）などのソフトウェア資産との有機的結合によって機能的に実現されるものであるが、ハードウェア資産およびオペレーティングシステムは汎用のものを利用できるから、前記説明のＩＤ情報や暗号鍵を利用したセキュリティ機能にとって欠くことのできない必須の事項は、実質的に、前述の「ユーザによるデータ書き込み処理」（図８参照）、「ユーザによるデータ再生処理」（図１０参照）または「ユーザによるディスクコピー処理」（図１２参照）などのプログラムに集約されているということがいえる。

【００８９】したがって、本発明に係るＩＤ情報や暗号鍵を利用したセキュリティ機能は、それらのプログラムのすべてまたはその要部を格納した、フロッピィディスク、光ディスク、コンパクトディスク、磁気テープ、ハードディスクまたは半導体メモリなどの記録媒体若しくはこれらの記録媒体を含む構成品（ユニット品や完成品または半完成品）を包含する。なお、その記録媒体または構成品は、それ自体が流通経路にのるものはもちろんのこと、ネットワーク上にあって記録内容だけを提供するものも含まれる。

【００９０】また、以上の説明では、ライトワンス型光ディスクとしてＣＤ－Ｒの例を示したが、これに限らない。例えば、ＤＶＤ（Digital Video DiscまたはDigital Versatile Disc）－Ｒも１回だけのデータ書き込みを

行うことができるから、もちろんライトワンス型光ディスクの仲間である。上記説明をＤＶＤ－Ｒに適用する場合、ＣＤ－ＲをＤＶＤ－Ｒと読み替えると共に、ＣＤ－Ｒ記録再生装置やＣＤ－Ｒライターをそれぞれ ＤＶＤ－Ｒ記録再生装置、ＤＶＤ－Ｒライターと読み替えればよい。

【００９１】

【発明の効果】請求項１記載の発明によれば、所定の製造者によって作られたライトワンス型光ディスクについてのみ、そのシステム領域の一部にセキュリティ対策のための情報が書き込まれる。したがって、特に秘匿を要するデータの保管や配布を行う際に、当該所定の製造者によって作られたライトワンス型光ディスクの使用を強制することができる。

【００９２】請求項２記載の発明によれば、データの再生時にその存在が無視される特定の領域（レーザ強度キャリブレーション用領域）にセキュリティ対策のための情報が書き込まれるため、当該領域はユーザに対して不可視であるばかりか、当業者にとってもレーザ強度キャリブレーション用として広く理解されているため、かかる専門知識を有する当業者に対しても不可視性を確保でき、セキュリティを保つことができる。

【００９３】請求項３記載の発明によれば、いずれもユーザからの直接的なアクセスが許容されていない領域にセキュリティ対策のための情報が書き込まれるため、当該情報をユーザからの隠し情報とすることができる。

【００９４】請求項４記載の発明によれば、ライトワンス型光ディスクの固体識別に基づくセキュリティ対策が可能となり、不正コピー等を防止し、データ再生時のセキュリティを向上することができる。

【００９５】請求項５記載の発明によれば、セキュリティ対策のための情報を利用したユーザ認証が可能となり、その認証結果を用いて不正ユーザを排除し、データ再生時のセキュリティを向上することができる。

【００９６】請求項６記載の発明によれば、セキュリティ対策のための情報を利用したユーザデータの暗号化が可能となり、万が一不正認証された場合でも、生データが露呈しないため、データの秘匿性を確保することができる。

【００９７】請求項７記載の発明によれば、セキュリティ対策のための情報を利用した暗号化データの復号が可能となり、万が一不正認証された場合でも、セキュリティ対策のための情報が読み取られない限り、生データが露呈せず、データの秘匿性を確保することができる。

【００９８】請求項８記載の発明によれば、所定の製造者によって作られたライトワンス型光ディスクについてのみ、そのシステム領域にセキュリティ対策のための情報が書き込まれる。したがって、特に秘匿を要するデータの保管や配布を行う際に、当該所定の製造者によって作られたライトワンス型光ディスクの使用を強制することができる。

【００９９】請求項９記載の発明によれば、マイクロコンピュータを含むハードウェア資産と該プログラムとの有機的結合によって前記アクセス手段、読み出し手段、判定手段および書き込み手段を実現することができる。

【図面の簡単な説明】

【図１】ライトワンス型光ディスクの外観図およびその要部拡大図である。

【図２】ＣＤ－Ｒの断面構造図である。

【図３】ＣＤ－Ｒに形成される案内溝（ウォッブルグルーブ）を示す模式図である。

【図４】ＣＤ－Ｒに案内溝を形成するために主としてディスクの製造段階で用いられる製造装置の構成図である。

【図５】ＣＤ－Ｒの各記録領域のフォーマット概念図である。

【図６】製造時にシステム領域に書き込まれるＩＤ情報と暗号鍵を含むデータフォーマットの例示構造図である。

【図７】ライトワンス型光ディスク記録再生装置の概略的なブロック構成図である。

【図８】ユーザ段階で実行されるデータ書き込み動作（ユーザによるデータ書き込み処理）を示すフローチャートである。

【図９】ユーザによるデータ書き込み処理のタイムランを示す図である。

【図１０】ユーザ段階で実行されるデータ再生動作（ユーザによるデータ再生処理）を示すフローチャートである。

【図１１】ユーザによるデータ再生処理のタイムランを示す図である。

【図１２】ユーザ段階で実行されるディスクコピー動作（ユーザによるディスクコピー処理）を示すフローチャートである。

【図１３】ユーザによるディスクコピー処理のタイムランを示す図である。

【符号の説明】

ＰＣＡ　Power Calibration Area（システム領域、レーザ強度キャリブレーション用領域）

ＰＭＡ　Program Memory Area（システム領域、セッション情報の一時格納用領域）

ＲＩ　リードイン（セッション情報格納用領域）

ＲＯ　リードアウト（ユーザ領域の終了位置を明示するための領域）

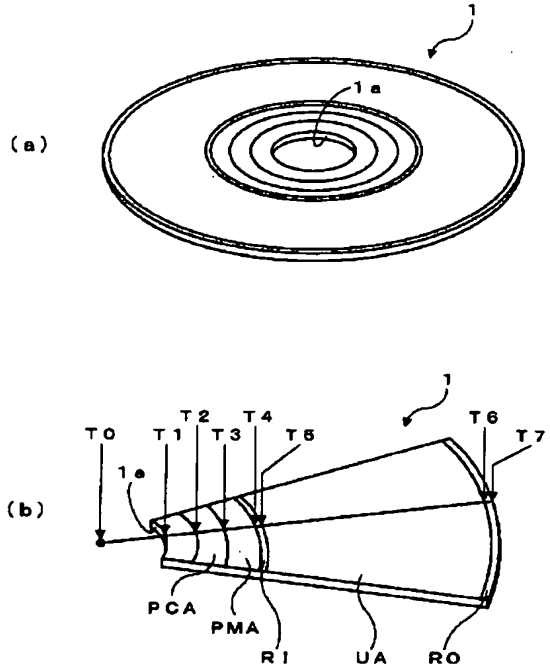
ＵＡ　ユーザエリア（ユーザ領域）

１　ＣＤ－Ｒ（ライトワンス型光ディスク）

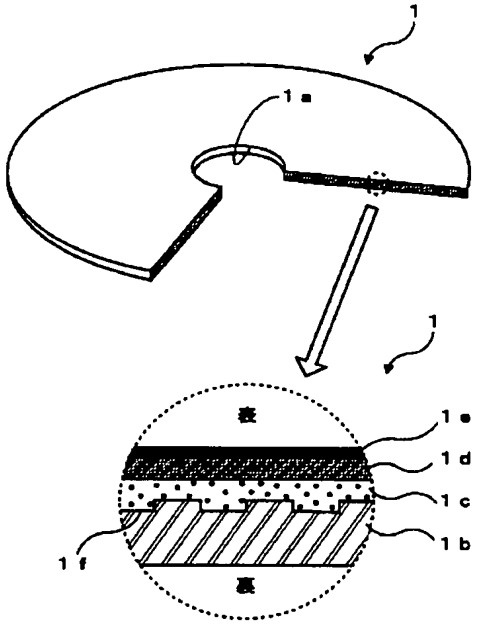
１０　ＣＤ－Ｒ記録再生装置（ライトワンス型光ディスク用記録装置）

２０　コントローラ（アクセス手段、読み出し手段、判定手段、書き込み手段）

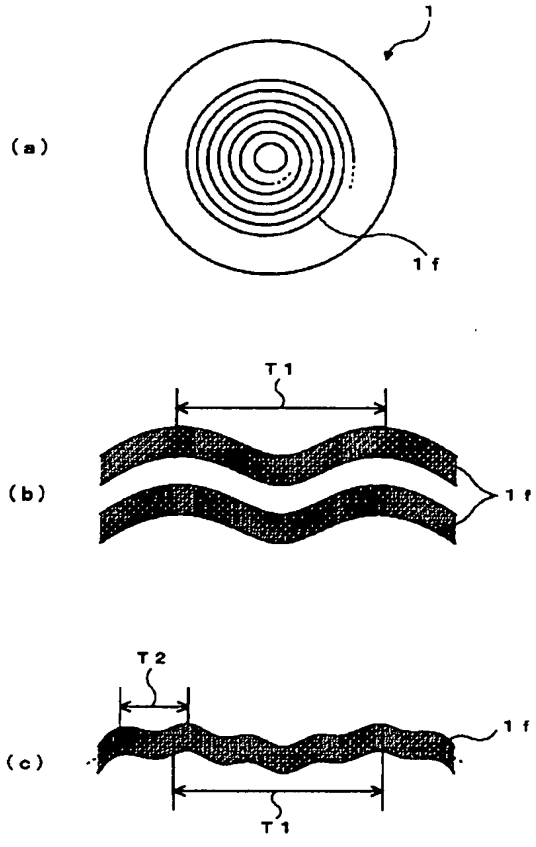
【図１】


(a)
1
1a
(b)
T0
T1
T2
T3
T4
T5
T6
T7
PCA
PMA
RI
UA
RO

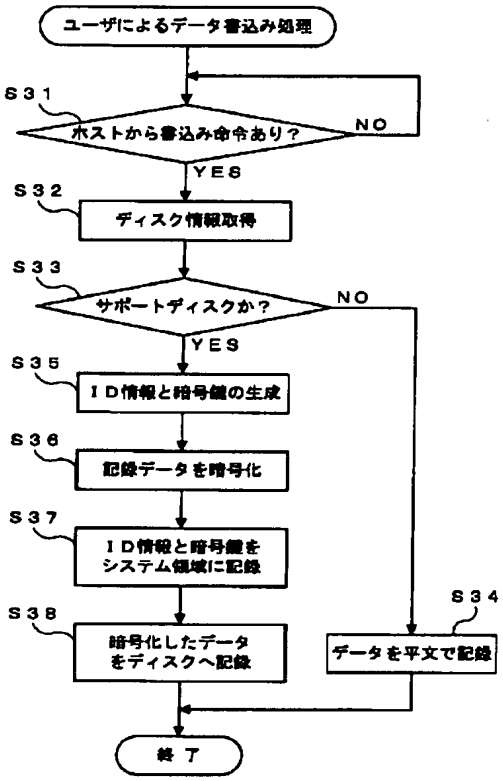
【図２】


1
1a
表
1e
1d
1c
1b
1f
裏

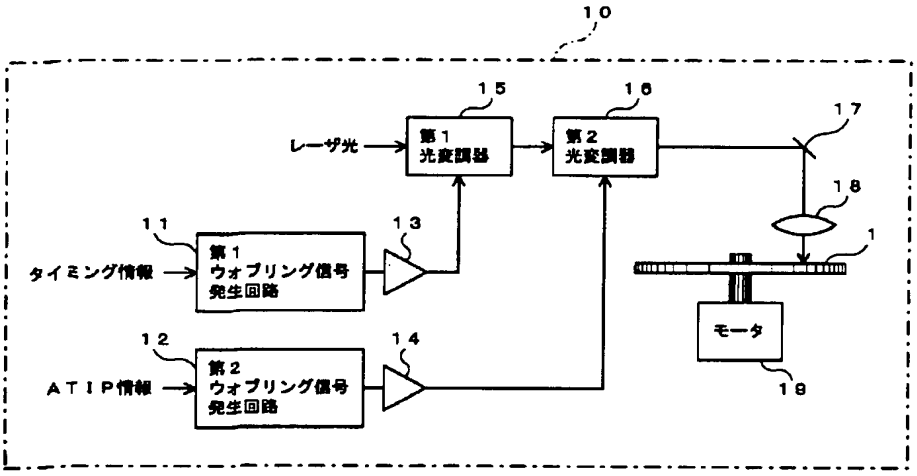
【図３】


(a)
1
1f
(b)
T1
1f
(c)
T2
1f
T1

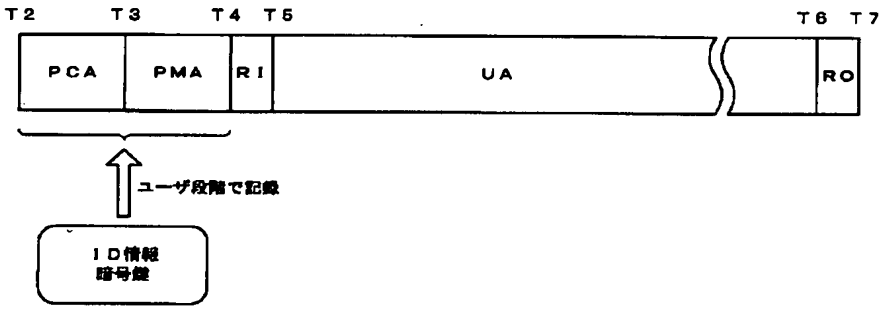
【図８】


ユーザによるデータ書込み処理
S31
ホストから書込み命令あり？
NO
YES
S32
ディスク情報取得
S33
サポートディスクか？
NO
YES
S35
ＩＤ情報と暗号鍵の生成
S36
記録データを暗号化
S37
ＩＤ情報と暗号鍵を
システム領域に記録
S38
暗号化したデータ
をディスクへ記録
S34
データを平文で記録
終了

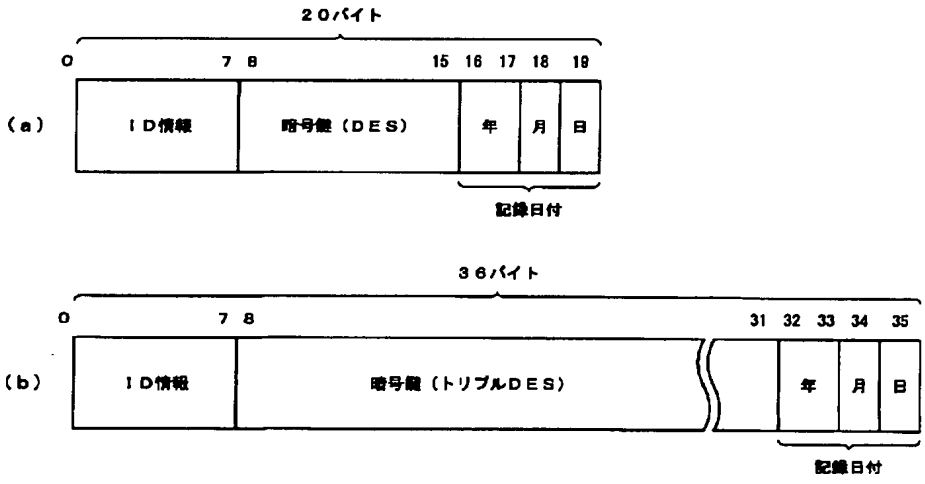
【図４】


10
15
16
17
レーザ光
第１
光変調器
第２
光変調器
18
11
13
1
タイミング情報
第１
ウォブリング信号
発生回路
モータ
12
14
ＡＴＩＰ情報
第２
ウォブリング信号
発生回路
19

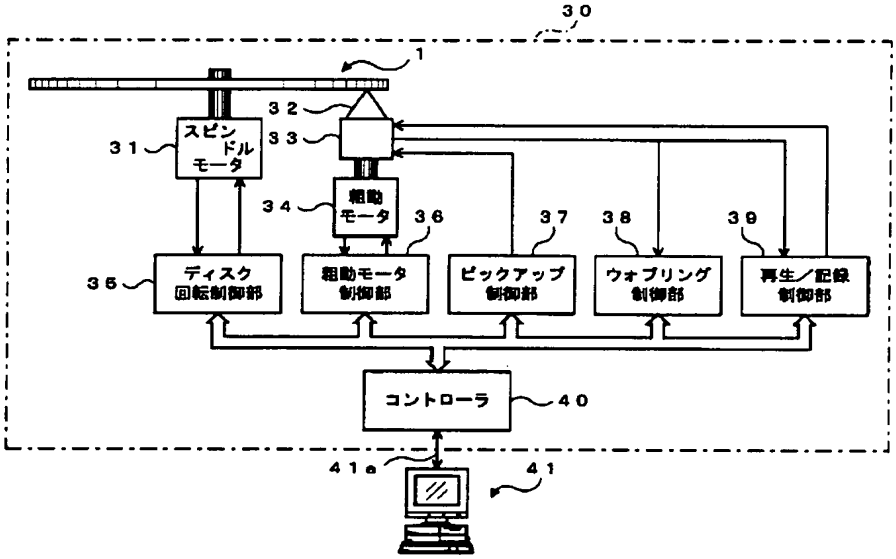
【図５】


T2
T3
T4
T5
T6
T7
PCA
PMA
RI
UA
RO
ユーザ段階で記録
ＩＤ情報
暗号鍵

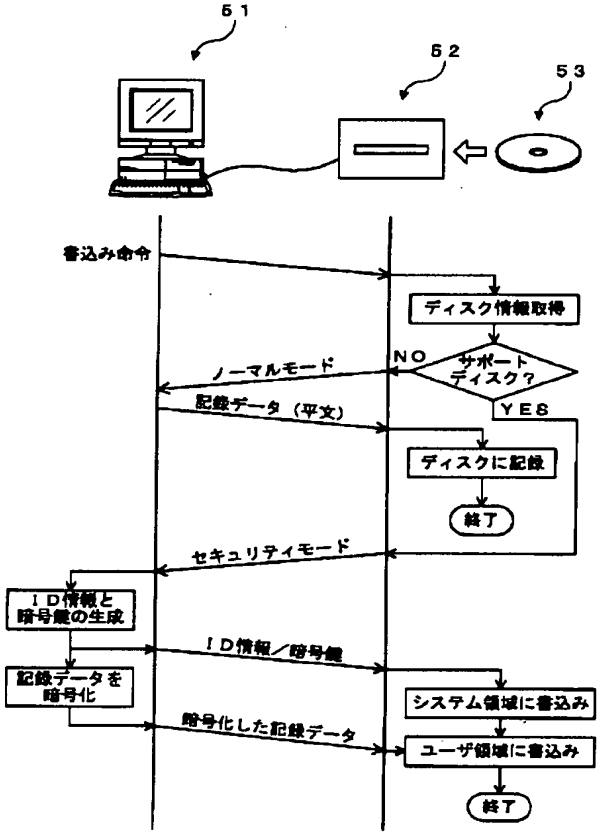
【図６】


２０バイト
0
7
8
15
16
17
18
19
(a)
ＩＤ情報
暗号鍵（ＤＥＳ）
年
月
日
記録日付
３６バイト
0
7
8
31
32
33
34
35
(b)
ＩＤ情報
暗号鍵（トリプルＤＥＳ）
年
月
日
記録日付

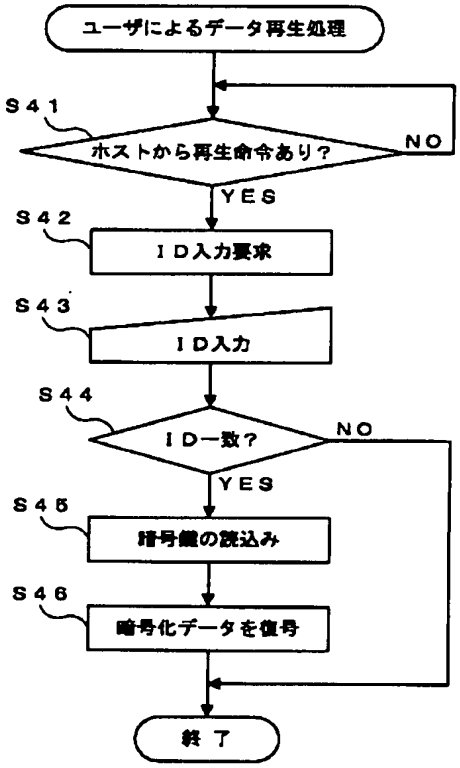
【図７】


30
1
32
31
スピンドルモータ
33
34
粗動モータ
36
37
38
39
35
ディスク回転制御部
粗動モータ制御部
ピックアップ制御部
ウォブリング制御部
再生／記録制御部
コントローラ
40
41a
41

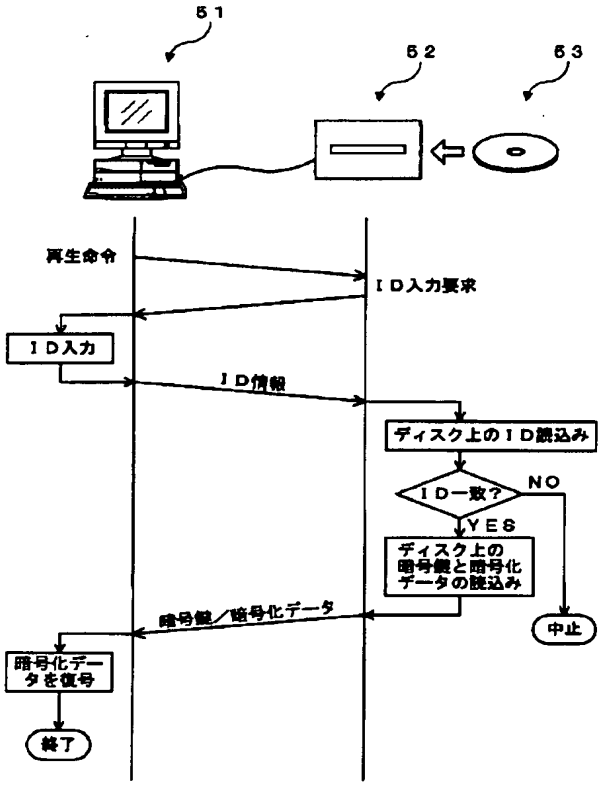
【図９】


51
52
53
書込み命令
ディスク情報取得
NO
サポートディスク？
YES
ノーマルモード
記録データ（平文）
ディスクに記録
終了
セキュリティモード
ＩＤ情報と暗号鍵の生成
ＩＤ情報／暗号鍵
記録データを暗号化
暗号化した記録データ
システム領域に書込み
ユーザ領域に書込み
終了

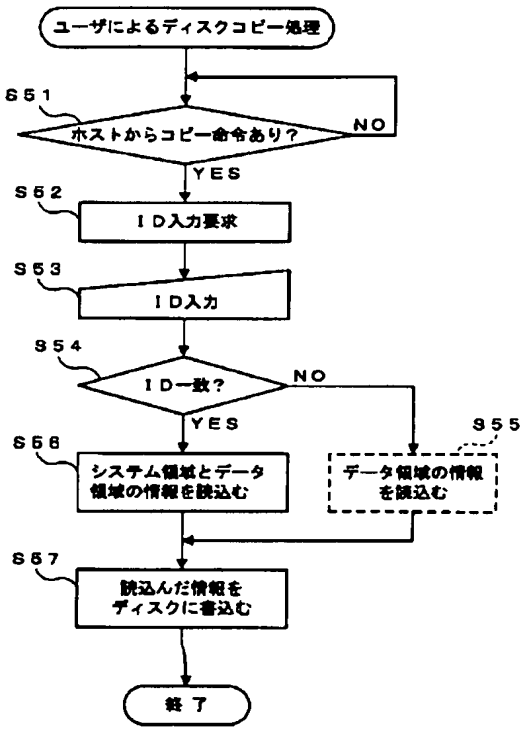
【図１０】


ユーザによるデータ再生処理
S41
ホストから再生命令あり？
NO
YES
S42
ＩＤ入力要求
S43
ＩＤ入力
S44
ＩＤ一致？
NO
YES
S45
暗号鍵の読込み
S46
暗号化データを復号
終了

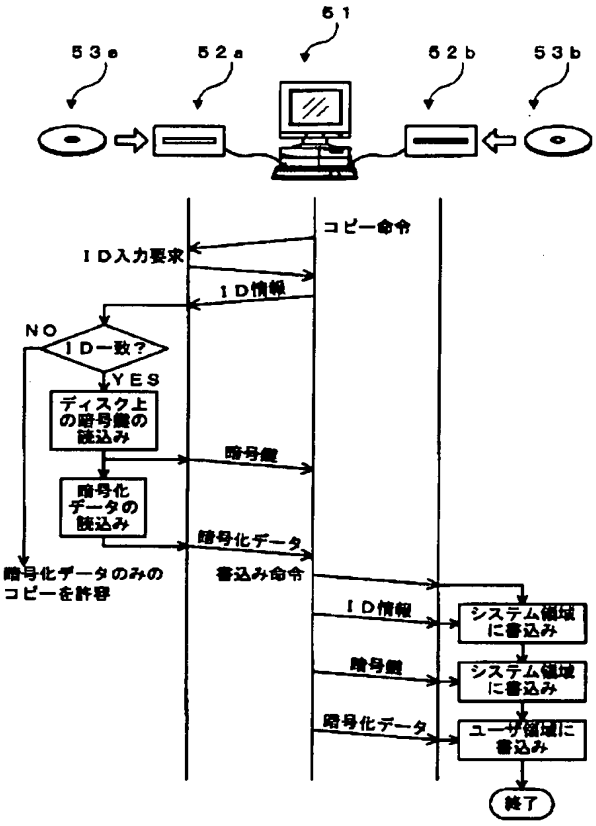
【図１１】


51
52
53
再生命令
ＩＤ入力要求
ＩＤ入力
ＩＤ情報
ディスク上のＩＤ読込み
ＩＤ一致？
NO
YES
ディスク上の暗号鍵と暗号化データの読込み
中止
暗号鍵／暗号化データ
暗号化データを復号
終了

【図１２】


ユーザによるディスクコピー処理
S51
ホストからコピー命令あり？
NO
YES
S52
ＩＤ入力要求
S53
ＩＤ入力
S54
ＩＤ一致？
NO
YES
S55
S56
システム領域とデータ領域の情報を読込む
データ領域の情報を読込む
S57
読込んだ情報をディスクに書込む
終了

【図１３】



フロントページの続き

(72)発明者　清水　洋信
東京都台東区上野６丁目16番20号　太陽誘電株式会社内

Ｆターム(参考)　5D044 AB01 AB05 AB07 BC05 CC04 DE49 DE50
5D066 DA12
5D090 AA01 BB03 CC14 DD02 DD05 FF24 GG32